PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-204698
(43)Date of publication of application : 09.08.1996

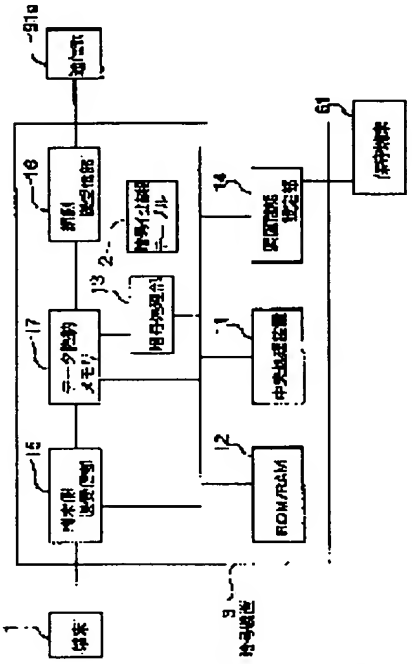
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G06F 15/00
G09C 1/00

(21)Application number : 07-008941
(22)Date of filing : 24.01.1995

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : TOKINIWA YASUHISA
WATANABE AKIRA
SENOO SHOICHIRO
YOKOYAMA YUKIO
NAGASHIMA NORIMITSU

(54) CIPHERING DEVICE

(57)Abstract:
PURPOSE: To attain communication with a ciphering key corresponding to sets of a terminal address and a data class in the data transmission reception between terminal equipments by using a terminal address of a communication opposite party and a registered ciphering key so as to apply ciphering processing to data included in the communication information.
CONSTITUTION: A ciphering information table 2 provided corresponding to a ciphering device 3 stores an IP(Internet Protocol) address of a communication opposite party, a data class and a ciphering key with cross reference. Then the ciphering device 3 decodes a TCP(Transmission Control Protocol) data part of an IP packet with the ciphering key registered in the ciphering information table 2 based on sets of the IP address and the data class when sets matching with those of the transmitter IP address and the data class in the received IP packet are in existence in the ciphering information table 2 and gives the IP packet to the terminal equipment. When the same sets are not in existence in the table 2, the device 3 does not conduct decoding and gives the IP packet to the terminal equipment.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－204698

(43)公開日　平成８年(1996)８月９日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/00				
9/10				
9/12				
Ｇ０６Ｆ　15/00	３３０　Ｚ	9364－5L		
			Ｈ０４Ｌ　9/00　Ｚ	

審査請求　未請求　請求項の数18　ＯＬ　（全 32 頁）　最終頁に続く

(21)出願番号　特願平7－8941

(22)出願日　平成７年(1995)１月24日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　時庭　康久
鎌倉市大船五丁目１番１号　三菱電機株式会社通信システム研究所内

(72)発明者　渡辺　晃
鎌倉市大船五丁目１番１号　三菱電機株式会社通信システム研究所内

(72)発明者　妹尾　尚一郎
鎌倉市大船五丁目１番１号　三菱電機株式会社通信システム研究所内

(74)代理人　弁理士　高田　守　（外４名）

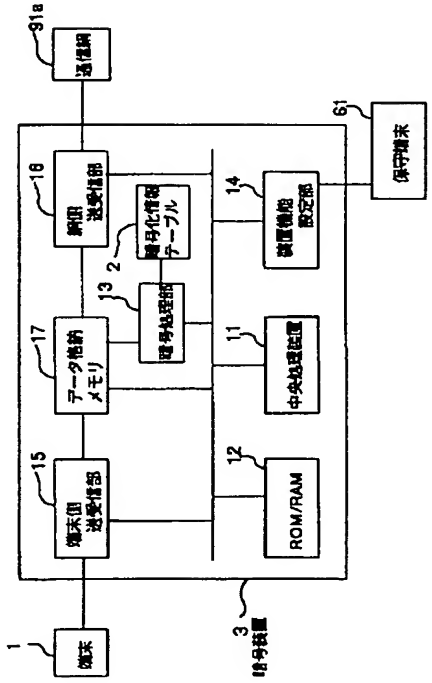
最終頁に続く

(54)【発明の名称】　暗号装置

(57)【要約】

【目的】　複数の端末間のデータ送受信において端末アドレスとデータ種別の組に対応した暗号鍵で通信できる暗号装置を得る。

【構成】　通信相手の端末アドレス、データ種別および暗号鍵を関連ずけて登録する暗号化情報登録手段を設け、端末からの通信相手の端末アドレス、データ種別および暗号対象のデータを含む通信情報を入力し、通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵とを用いて、通信情報に含まれるデータを暗号処理して出力する。



1

【特許請求の範囲】

【請求項１】　以下の構成要素を有する暗号装置。

１．通信相手の端末アドレス、データ種別および暗号対象のデータを含む通信情報を入力する入力手段、

２．前記通信相手の端末アドレス、前記データ種別および暗号鍵を関連ずけて登録する暗号化情報登録手段、

３．前記通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて前記通信情報に含まれるデータを暗号処理する暗号処理手段、

４．前記暗号処理した前記通信情報を出力する出力手段。

【請求項２】　以下の構成要素を有する暗号装置。

１．通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段、

２．前記通信相手の端末アドレスと複数の暗号鍵を関連ずけて登録する暗号化情報登録手段、

３．前記通信情報に含まれる通信相手の端末アドレスに対応して前記暗号化情報登録手段に登録されている前記複数の暗号鍵を用いて前記通信情報に含まれるデータを複数回暗号処理する暗号処理手段、

４．前記暗号処理した前記通信情報を出力する出力手段。

【請求項３】　前記入力手段はデータ種別を含む前記通信情報を入力し、前記暗号化情報登録手段は前記通信相手の端末アドレスおよび複数の暗号鍵の他に前記データ種別を関連ずけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの他に前記データ種別に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項２に記載の暗号装置。

【請求項４】　以下の構成要素を有する暗号装置。

１．送信元端末アドレス、宛先端末アドレス、暗号対象のデータを含む通信情報を入力する入力手段、

２．前記送信元端末アドレス、前記宛先端末アドレスおよび暗号鍵を関連ずけて登録する暗号化情報登録手段、

３．前記通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて前記通信情報に含まれるデータを暗号処理する暗号処理手段、

４．前記暗号処理した前記通信情報を出力する出力手段。

【請求項５】　以下の構成要素を有する暗号装置。

１．第１の通信網および第２の通信網からの、送信元端末アドレス、宛先端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段、

２．前記送信元端末アドレス、前記宛先端末アドレスおよび暗号鍵を関連ずけて登録する暗号化情報登録手段、

３．前記通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して前記暗号化情報登録手段に登録

2

されている前記暗号鍵を用いて、前記第２通信網からの前記通信情報に含まれるデータを暗号化または、前記第１通信網からの前記通信情報に含まれるデータを復号する暗号処理手段、

４．前記暗号化または復号した前記通信情報を出力する出力手段。

【請求項６】　前記入力手段はデータ種別を含む前記通信情報を入力し、前記暗号化情報登録手段は前記送信元端末アドレス、前記宛先端末アドレス、および暗号鍵の他に前記データ種別を関連ずけて登録し、前記暗号処理手段は前記送信元端末アドレスと前記宛先端末アドレスの他に前記データ種別にも対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項４または請求項５に記載の暗号装置。

【請求項７】　以下の構成要素を有する暗号装置。

１．通信相手の端末アドレスと暗号対象のデータを含む前記通信情報を入力する入力手段、

２．前記通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵とを関連ずけて登録する暗号化情報登録手段、

３．前記通信情報に含まれる前記通信相手の端末アドレスに対応して前記暗号化情報登録手段に登録されている前記第一の暗号鍵を用いて前記通信相手への前記通信情報に含まれるデータを暗号化または、前記第二の暗号鍵を用いて前記通信相手からの前記通信情報に含まれるデータを復号する暗号処理手段、

４．前記暗号化または復号した前記通信情報を出力する出力手段。

【請求項８】　前記入力手段はデータ種別を含む前記通信情報を入力し、前記暗号化情報登録手段は前記通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵の他に前記データ種別とを関連ずけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの他に前記データ種別に対応して前記暗号化情報登録手段に登録されている前記第一の暗号鍵を用いて暗号化または、前記第二の暗号鍵を用いて復号することを特徴とする請求項７に記載の暗号装置。

【請求項９】　以下の構成要素を有する暗号装置。

１．通信相手の端末アドレス、データ種別と暗号対象のデータを含む前記通信情報を入力する入力手段、

２．前記通信相手の端末アドレス、前記データ種別、暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連ずけて登録する暗号化情報登録手段、

３．前記通信情報に含まれる前記通信相手の端末アドレスと前記データ種別に対応して前記暗号化情報登録手段に登録されている前記第一の複数の暗号鍵を用いて前記通信相手への前記通信情報に含まれるデータを複数回暗号化または、前記第二の複数の暗号鍵を用いて前記通信

相手からの前記通信情報に含まれるデータを複数回復号する暗号処理手段、

４．前記暗号化または復号した前記通信情報を出力する出力手段。

【請求項１０】　前記暗号化情報登録手段は前記送信元端末アドレスと前記宛先端末アドレスに複数の暗号鍵を関連ずけて登録し、前記暗号処理手段は前記複数の暗号鍵を用いて前記通信情報に含まれるデータを複数回暗号処理することを特徴とする請求項４に記載の暗号装置。

【請求項１１】　前記暗号化情報登録手段は前記送信元端末アドレスと前記宛先端末アドレスに複数の暗号鍵を関連ずけて登録し、前記暗号処理手段は前記複数の暗号鍵を用いて、前記第２通信網からの前記通信情報に含まれるデータを複数回暗号化または、前記第１通信網からの前記通信情報に含まれるデータを複数回復号することを特徴とする請求項５に記載の暗号装置。

【請求項１２】　前記暗号化情報登録手段は前記通信相手の端末アドレスに暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連ずけて登録し、前記暗号処理手段は前記第一の複数の暗号鍵を用いて前記通信相手への前記通信情報に含まれるデータを複数回暗号化または、前記第二の複数の暗号鍵を用いて前記通信相手からの前記通信情報に含まれるデータを複数回復号することを特徴とする請求項７に記載の暗号装置。

【請求項１３】　以下の構成要素を有する暗号装置。

１．送信元端末アドレス、宛先端末アドレス、データ種別、暗号対象のデータを含む通信情報を入力する入力手段、

２．前記送信元端末アドレス、前記宛先端末アドレス、前記データ種別および複数の暗号鍵を関連ずけて登録する暗号化情報登録手段、

３．前記通信情報に含まれる送信元端末アドレス、宛先端末アドレス、データ種別に対応して前記暗号化情報登録手段に登録されている前記複数の暗号鍵を用いて前記通信情報に含まれるデータを複数回暗号処理する暗号処理手段、

４．前記暗号処理した前記通信情報を出力する出力手段。

【請求項１４】　前記暗号化情報登録手段は複数桁からなる前記通信相手の端末アドレスの一部の桁をデータ種別と前記暗号鍵に関連ずけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの一部の桁と前記データ種別に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項１に記載の暗号装置。

【請求項１５】　前記暗号化情報登録手段は複数桁からなる前記通信相手の端末アドレスの一部の桁を前記暗号鍵に関連ずけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの一部の桁に対応して前記暗号化情報

登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項２に記載の暗号装置。

【請求項１６】　前記暗号化情報登録手段は複数桁からなる前記送信元端末アドレスまたは前記宛先端末アドレスの一部の桁を前記暗号鍵に関連ずけて登録し、前記暗号処理手段は前記送信元端末アドレスまたは前記宛先端末アドレスの一部の桁に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号処理することを特徴とする請求項４に記載の暗号装置。

【請求項１７】　前記暗号化情報登録手段は複数桁からなる前記送信元端末アドレスまたは前記宛先端末アドレスの一部の桁を前記暗号鍵に関連ずけて登録し、前記暗号処理手段は前記送信元端末アドレスまたは前記宛先端末アドレスの一部の桁に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号化または復号することを特徴とする請求項５に記載の暗号装置。

【請求項１８】　前記暗号化情報登録手段は複数桁からなる前記通信相手の端末アドレスの一部の桁を前記暗号鍵に関連ずけて登録し、前記暗号処理手段は前記通信相手の端末アドレスの一部の桁に対応して前記暗号化情報登録手段に登録されている前記暗号鍵を用いて暗号化または復号することを特徴とする請求項７に記載の暗号装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、通信網における暗号通信に関するものである。

【０００２】

【従来の技術】従来より暗号方式には秘密暗号方式と呼ばれるものがあり、例えば６４ビットの鍵を用いたＡＮＳＩ（アメリカ国規格協会）の標準であるＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）方式や日本電信電話株式会社の登録商標であるＦＥＡＬ（Ｆａｓｔ　ｄａｔａ　Ｅｎｃｉｐｈｅｒｍｅｎｔ　ＡＬｇｏｒｉｔｈｍ）などがある。また、通信網における暗号通信に関する暗号装置や暗号通信方式として、宛先の端末に対応した鍵を用いた暗号通信について、特開昭61-81044、特開平4-86041、特開平4-297155、特開平4-326222、特開平5-244153などの数多くの例が考案されている。図１９は例えば特開平4-297155号公報に示された従来の暗号装置の実施例を示す構成図である。図１９において、１は端末、３は暗号装置、７０２はアドレス情報を保持するアドレス保持部、７０３は第１分岐合成回路、７０４は変調復調器、７０５は第２分岐合成回路、７０７はトランシーバ、９１ａは通信網である。

【０００３】次に動作について説明する。図２０、図２１は従来の暗号装置の処理手順を示す図である。端末１から暗号化の対象となるパケットの宛先アドレスとその暗号系列を表す暗号鍵をアドレス保持部７０２に送り、アドレス保持部７０２がその宛先アドレスと暗号鍵を対

応させてメモリに保持することによって初期設定を行う。

【０００４】図２０は送信の処理手順を示し、ステップ７１４で端末１が暗号装置３にパケットを送る。ステップ７１５で、暗号装置３の第１分岐合成回路７０３がアドレス保持部７０２にそのパケットの宛先が保持されているか参照し、ステップ７１６で、宛先アドレスが保持されているならば、ステップ７１７に進み、第１分岐合成回路７０３がパケットを変調復調器７０４に送る。ステップ７３５で変調復調器７０４がアドレス保持部７０２からパケットの宛先アドレスの暗号鍵を受け取り、ステップ７３６で、変調復調器７０４が暗号鍵に従ってパケットを暗号化し、ステップ７１９で、変調復調器７０４がそのパケットを第２分岐合成回路７０５に送りステップ７２１に進む。ステップ７１６で、アドレス保持部７０２に宛先アドレスが保持されていなければ、ステップ７２０に進み、第１分岐合成回路７０３がパケットを第２分岐構成回路７０５に送る。次に、ステップ７２１で、第２分岐合成回路７０５がパケットを通信網９１ａに送る。

【０００５】図２１は受信の処理手順を示し、ステップ７２４で、通信網９１ａから暗号装置３にパケットを送られ、ステップ７２５で、暗号装置３の第２分岐合成回路７０５がアドレス保持部７０２にパケットの送信元アドレスが保持されているか参照し、ステップ７２６で、送信元アドレスが保持されているならば、ステップ７２７に進み、第２分岐合成回路７０５がパケットを変調復調器７０４に送り、ステップ７３５で変調復調器７０４がアドレス保持部７０２からパケットの送信元アドレスの暗号鍵を受け取り、ステップ７３７で、暗号鍵に従って暗号を復号し、ステップ７２９で、復号されたパケットを第１分岐合成回路７０３に送り、ステップ７３１に進む。ステップ７２６で、アドレス保持部７０２に送信元アドレスが保持されていなければ７３０に進み、第２分岐合成回路７０５がパケットを第１分岐合成回路７０３に送り、ステップ７３１で、第１分岐合成回路７０３がパケットを端末１に送る。

【０００６】通信網９１ａに接続された複数の端末１間の通信で、暗号装置３のパケット送受信において共通の暗号鍵を用いて前記暗号化・復号を行うことにより暗号閉域通信が可能となる。

【０００７】

【発明が解決しようとする課題】従来の暗号装置は以上のように通信相手対応に暗号鍵を用いるので、ある相手端末にパケットを送る場合、データ種別に関係なくすべてのデータを同じ暗号鍵で暗号化・復号を行っていて、データ種別によっては暗号化する必要がないデータまで暗号化していたため、暗号化・復号に掛かる無駄な遅延時間が発生していた。また、複数の相手端末と暗号通信する場合、一つの暗号鍵を共用すると暗号鍵が漏れる可能性が高まり、暗号鍵の強度が弱い欠点があった。また、相互に暗号通信の必要のない安全域のネットワークに属する端末と暗号通信を必要とする危険域のネットワークに属する端末が通信する場合、安全域のネットワーク内の端末ごとに暗号装置を設ければ暗号通信が可能であるが多くの費用を要した。

【０００８】また、２つの端末間のパケットは、送信／受信に係わらず同一の暗号鍵を用いて暗号化・復号を行っていたので、どちらかの方向の暗号が破られれば、他方向の暗号が破られるため暗号強度が弱いという問題があった。また、端末アドレスの上位桁が同一の端末がネットワークまたはサブネットワークを構成し、ネットワーク内の各端末が同じ暗号鍵を用いて、他のネットワークの端末と暗号通信する場合でも、通信相手と暗号鍵との関係を示す情報を端末毎に登録しなければならず、保守の労力が大きかった。

【０００９】この発明は前記のような問題点を解消するためになされたもので、第一の目的は、端末間のデータ送受信において端末アドレスとデータ種別の組に対応した暗号鍵で通信できる暗号装置を得ることを目的とする。

【００１０】第二の目的は、端末間のデータ送受信において暗号強度の異なる鍵で通信できる暗号装置を得ることを目的とする。

【００１１】第三の目的は、安全域内では暗号通信する必要のない通信網に属する端末が、暗号通信を必要とする危険域内の通信網に属する端末と通信する際、危険域内は暗号通信できる暗号装置を得ることを目的とする。

【００１２】第四の目的は、端末間のデータ送受信においてに送信用と受信用とで別の暗号鍵で通信できる暗号装置を得ることを目的とする。

【００１３】第五の目的は、一つの通信網に属している端末に暗号鍵を設定するための操作労力を軽減することを目的とする。

【００１４】

【課題を解決するための手段】第一の発明に係わる暗号装置は、通信相手の端末アドレス、データ種別および暗号対象のデータを含む通信情報を入力する入力手段と、通信相手の端末アドレス、データ種別および暗号鍵を関連ずけて登録する暗号化情報登録手段と、通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて通信情報に含まれるデータを暗号処理する暗号処理手段と、暗号処理した通信情報を出力する出力手段とを備えたものである。

【００１５】第二の発明に係わる暗号装置は、通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段と、通信相手の端末アドレスと複数の暗号鍵を関連ずけて登録する暗号化情報登録手段と、通信情報に含まれる通信相手の端末アドレスに対応して暗号

化情報登録手段に登録されている複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理する暗号処理手段と、暗号処理した通信情報を出力する出力手段とを備えたものである。

【００１６】第三の発明に係わる入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレスおよび複数の暗号鍵の他にデータ種別を関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの他にデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【００１７】第四の発明に係わる暗号装置は、送信元端末アドレス、宛先端末アドレス、暗号対象のデータを含む通信情報を入力する入力手段と、送信元端末アドレス、宛先端末アドレスおよび暗号鍵を関連ずけて登録する暗号化情報登録手段と、通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して暗号化情報登録手段に登録されている暗号鍵を用いて通信情報に含まれるデータを暗号処理する暗号処理手段と、暗号処理した通信情報を出力する出力手段とを備えたものである。

【００１８】第五の発明に係わる暗号装置は、第１の通信網および第２の通信網からの、送信元端末アドレス、宛先端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段と、送信元端末アドレス、宛先端末アドレスおよび暗号鍵を関連ずけて登録する暗号化情報登録手段と、通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して暗号化情報登録手段に登録されている暗号鍵を用いて、第２通信網からの通信情報に含まれるデータを暗号化または、第１通信網からの通信情報に含まれるデータを復号する暗号処理手段と、暗号化または復号した通信情報を出力する出力手段とを備えたものである。

【００１９】第六の発明に係わる入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は送信元端末アドレス、宛先端末アドレス、および暗号鍵の他にデータ種別を関連ずけて登録し、暗号処理手段は送信元端末アドレスと宛先端末アドレスの他にデータ種別にも対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【００２０】第七の発明に係わる暗号装置は、通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力する入力手段と、通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵とを関連ずけて登録する暗号化情報登録手段と、通信情報に含まれる通信相手の端末アドレスに対応して暗号化情報登録手段に登録されている第一の暗号鍵を用いて通信相手への通信情報に含まれるデータを暗号化または、第二の暗号鍵を用いて通信相手からの通信情報に含まれるデータを復号する暗号処理手段と、暗号化または復号した通信情報を出力する出力手段とを備えたものである。

【００２１】第八の発明に係わる入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵の他にデータ種別とを関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの他にデータ種別に対応して暗号化情報登録手段に登録されている第一の暗号鍵を用いて暗号化または、第二の暗号鍵を用いて復号するものである。

【００２２】第九の発明に係わる暗号装置は、通信相手の端末アドレス、データ種別と暗号対象のデータを含む通信情報を入力する入力手段と、通信相手の端末アドレス、データ種別、暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連ずけて登録する暗号化情報登録手段と、通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して暗号化情報登録手段に登録されている第一の複数の暗号鍵を用いて通信相手への通信情報に含まれるデータを複数回暗号化または、第二の複数の暗号鍵を用いて通信相手からの通信情報に含まれるデータを複数回復号する暗号処理手段と、暗号化または復号した通信情報を出力する出力手段とを備えたものである。

【００２３】第十の発明に係わる暗号化情報登録手段は、送信元端末アドレスと宛先端末アドレスに複数の暗号鍵を関連ずけて登録し、暗号処理手段は複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理するものである。

【００２４】第十一の発明に係わる暗号化情報登録手段は送信元端末アドレスと宛先端末アドレスに複数の暗号鍵を関連ずけて登録し、暗号処理手段は複数の暗号鍵を用いて、第２通信網からの通信情報に含まれるデータを複数回暗号化または、第１通信網からの通信情報に含まれるデータを複数回復号するものである。

【００２５】第十二の発明に係わる暗号化情報登録手段は通信相手の端末アドレスに暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連ずけて登録し、暗号処理手段は第一の複数の暗号鍵を用いて通信相手への通信情報に含まれるデータを複数回暗号化または、第二の複数の暗号鍵を用いて通信相手からの通信情報に含まれるデータを複数回復号するものである。

【００２６】第十三の発明に係わる暗号装置は、送信元端末アドレス、宛先端末アドレス、データ種別、暗号対象のデータを含む通信情報を入力する入力手段と、送信元端末アドレス、宛先端末アドレス、データ種別および複数の暗号鍵を関連ずけて登録する暗号化情報登録手段と、通信情報に含まれる送信元端末アドレス、宛先端末アドレス、データ種別に対応して暗号化情報登録手段に登録されている複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理する暗号処理手段と、暗号処理した通信情報を出力する出力手段とを備えたものであ

る。

【００２７】第十四の発明に係わる暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁をデータ種別と暗号鍵に関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁とデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【００２８】第十五の発明に係わる暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁を暗号鍵に関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【００２９】第十六の発明に係わる暗号化情報登録手段は複数桁からなる送信元端末アドレスまたは宛先端末アドレスの一部の桁を暗号鍵に関連ずけて登録し、暗号処理手段は送信元端末アドレスまたは宛先端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理するものである。

【００３０】第十七の発明に係わる暗号化情報登録手段は複数桁からなる送信元端末アドレスまたは宛先端末アドレスの一部の桁を暗号鍵に関連ずけて登録し、暗号処理手段は送信元端末アドレスまたは宛先端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号化または復号するものである。

【００３１】第十八の発明に係わる暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁を暗号鍵に関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号化または復号するものである。

【００３２】

【作用】第一の発明において、入力手段が通信相手の端末アドレス、データ種別および暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段が通信相手の端末アドレス、データ種別および暗号鍵を関連ずけて登録する。そして、暗号処理手段が、通信情報に含まれる通信相手の端末アドレスと、データ種別に対応して暗号化情報登録手段に登録されている暗号鍵とを用いて通信情報に含まれるデータを暗号処理し、出力手段が暗号処理した通信情報を出力する。

【００３３】第二の発明において、入力手段は通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレスと複数の暗号鍵を関連ずけて登録する。そして、暗号処理手段は通信情報に含まれる通信相手の端末アドレスに対応して暗号化情報登録手段に登録されている複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理し、出力手段は暗号処理した通信情報を出力する。

【００３４】第三の発明において、　入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレスおよび複数の暗号鍵の他にデータ種別を関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの他にデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【００３５】第四の発明において、入力手段は送信元端末アドレス、宛先端末アドレス、暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段が送信元端末アドレス、宛先端末アドレスおよび暗号鍵を関連ずけて登録する。そして、暗号処理手段は通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して暗号化情報登録手段に登録されている暗号鍵を用いて通信情報に含まれるデータを暗号処理し、出力手段は暗号処理した通信情報を出力する。

【００３６】第五の発明において、入力手段は第１の通信網および第２の通信網からの、送信元端末アドレス、宛先端末アドレスと暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は送信元端末アドレス、宛先端末アドレスおよび暗号鍵を関連ずけて登録する。そして、暗号処理手段が通信情報に含まれる送信元端末アドレスと宛先端末アドレスに対応して暗号化情報登録手段に登録されている暗号鍵を用いて、第２通信網からの通信情報に含まれるデータを暗号化または、第１通信網からの通信情報に含まれるデータを復号し、出力手段が暗号化または復号した通信情報を出力する。

【００３７】第六の発明において、入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は送信元端末アドレス、宛先端末アドレス、および暗号鍵の他にデータ種別を関連ずけて登録し、暗号処理手段は送信元端末アドレスと宛先端末アドレスの他にデータ種別にも対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【００３８】第七の発明において、入力手段は通信相手の端末アドレスと暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵とを関連ずけて登録する。そして、暗号処理手段は通信情報に含まれる通信相手の端末アドレスに対応して暗号化情報登録手段に登録されている第一の暗号鍵を用いて通信相手への通信情報に含まれるデータを暗号化または、第二の暗号鍵を用いて通信相手からの通信情報に含まれるデータを復号し、出力手段は暗号化または復号した通信情報を出力する。

【００３９】第八の発明において、入力手段はデータ種別を含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレス、暗号化に用いる第一の暗号鍵および復号に用いる第二の暗号鍵の他にデータ種別とを関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの他にデータ種別に対応して暗号化情報登録手段に登録されている第一の暗号鍵を用いて暗号化または、第二の

暗号鍵を用いて復号することを特徴とする。

【００４０】第九の発明において、入力手段は通信相手の端末アドレス、データ種別と暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は通信相手の端末アドレス、データ種別、暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連ずけて登録する。そして、暗号処理手段は通信情報に含まれる通信相手の端末アドレスとデータ種別に対応して暗号化情報登録手段に登録されている第一の複数の暗号鍵を用いて通信相手への通信情報に含まれるデータを複数回暗号化または、第二の複数の暗号鍵を用いて通信相手からの通信情報に含まれるデータを複数回復号し、出力手段は暗号化または復号した通信情報を出力する。

【００４１】第十の発明において、暗号化情報登録手段は送信元端末アドレスと宛先端末アドレスに複数の暗号鍵を関連ずけて登録し、暗号処理手段は複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理する。

【００４２】第十一の発明において、暗号化情報登録手段は送信元端末アドレスと宛先端末アドレスに複数の暗号鍵を関連ずけて登録し、暗号処理手段は複数の暗号鍵を用いて、第２通信網からの通信情報に含まれるデータを複数回暗号化または、第１通信網からの通信情報に含まれるデータを複数回復号する。

【００４３】第十二の発明において、暗号化情報登録手段は通信相手の端末アドレスに暗号化に用いる第一の複数の暗号鍵および復号に用いる第二の複数の暗号鍵とを関連ずけて登録し、暗号処理手段は第一の複数の暗号鍵を用いて通信相手への通信情報に含まれるデータを複数回暗号化または、第二の複数の暗号鍵を用いて通信相手からの通信情報に含まれるデータを複数回復号する。

【００４４】第十三の発明において、入力手段は送信元端末アドレス、宛先端末アドレス、データ種別、暗号対象のデータを含む通信情報を入力し、暗号化情報登録手段は送信元端末アドレス、宛先端末アドレス、データ種別および複数の暗号鍵を関連ずけて登録する。そして、暗号処理手段は通信情報に含まれる送信元端末アドレス、宛先端末アドレス、データ種別に対応して暗号化情報登録手段に登録されている複数の暗号鍵を用いて通信情報に含まれるデータを複数回暗号処理し、出力手段は暗号処理した通信情報を出力する。

【００４５】第十四の発明において、暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁をデータ種別と暗号鍵に関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁とデータ種別に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【００４６】第十五の発明において、暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁を暗号鍵に関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【００４７】第十六の発明において、暗号化情報登録手段は複数桁からなる送信元端末アドレスまたは宛先端末アドレスの一部の桁を暗号鍵に関連ずけて登録し、暗号処理手段は送信元端末アドレスまたは宛先端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号処理する。

【００４８】第十七の発明において、暗号化情報登録手段は複数桁からなる送信元端末アドレスまたは宛先端末アドレスの一部の桁を暗号鍵に関連ずけて登録し、暗号処理手段は送信元端末アドレスまたは宛先端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号化または復号する。

【００４９】第十八の発明において、暗号化情報登録手段は複数桁からなる通信相手の端末アドレスの一部の桁を暗号鍵に関連ずけて登録し、暗号処理手段は通信相手の端末アドレスの一部の桁に対応して暗号化情報登録手段に登録されている暗号鍵を用いて暗号化または復号する。

【００５０】

【実施例】

実施例１．本実施例は端末対応だけではなく、端末とデータ種別の組に対応して暗号鍵を設けようとするもので、暗号装置の構成を図１に示す。図において、１は端末、３は暗号装置、１１は各種の演算制御を行う中央処理装置、１２はプログラムおよびワーキング用のメモリとして使用するＲＯＭ／ＲＡＭ、１３は暗号処理部で、暗号化情報テーブル２を保持しデータの暗号化／復号を行う。１４は暗号鍵の設定を行う装置機能設定部、１５は端末側送受信部、１６は網側送受信部、１７はデータ格納メモリ、６１は暗号鍵を入力するために用いる保守端末、９１ａは通信網である。

【００５１】図２は、暗号通信システムの構成例を示す図であり、図において、１ａ～１ｈは端末、３ａ～３ｅは端末１ａ～１ｅ対応に設けた暗号装置、９１ａは通信網である。なお、１８３ａは端末１ａ、１ｂ、１ｃが所属している通信閉域であり、１８３ｂは端末１ａ、１ｂ、１ｄ、１ｅが所属している通信閉域である。図３は、送受信データとしてのＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケットの構成を示す図であり、図において、４０１は送信元ＩＰアドレス部、４０２は宛先ＩＰアドレス部、４１１はＩＰヘッダ部、４１２はＩＰデータ部、４３１はデータ種別を収容するデータ種別部、４４１はＴＣＰヘッダ部、４４２はＴＣＰデータ部、４４５はＩＰパケットである。

【００５２】なお、端末を識別するための端末アドレスとして、ここではＩＰアドレスを用いて説明するがＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスや他のネットワークプロトコルのアドレスであって

もよい。また、ＩＰアドレスは、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）の通信手順で用いられている端末を識別するための４バイトの情報である。また、データ種別部４３１には、データ種別が入るが、ユーザアプリケーションを識別するポート番号であってもよい。

【００５３】図４は、暗号装置３対応に設けた暗号化情報テーブル２の内容を例示するもので、図において、２ａ～２ｅは暗号装置３ａ～３ｅ対応に設けた暗号化情報テーブルで、通信相手のＩＰアドレス、データ種別および暗号鍵を一組とし関連ずけて記憶する。そして、通信相手のＩＰアドレスとデータ種別の組と一致するものが暗号化情報テーブル２内にあるか調べ、あるならその組に対応する暗号鍵を用いて暗号化または復号することを意味し、一致するものがなければ、暗号化または復号しないことを意味する。暗号化情報テーブル２内の３１ａ～３１ｅは端末を識別するためのＩＰアドレスで、各々端末１ａ～１ｅが対応する。

【００５４】３２６ａ、３２６ｂはデータ種別で、３４１ａ、３４１ｂは暗号鍵である。本実施例ではデータ種別３２６ａは暗号鍵３４１ａに、データ種別３２６ｂは暗号鍵３４１ｂに対応させている。なお、図４は図２の通信網構成で暗号通信を行うために各暗号装置３の暗号化情報テーブル２に登録する内容を例示たもので、端末１ａに対応する暗号化情報テーブル２ａは暗号通信相手として端末１ｂ、１ｃ、１ｄ，１ｅがあり、端末１ｂに対応するＩＰアドレス３１ｂにデータ種別３２６ａと暗号鍵３４１ａおよびデータ種別３２６ｂと暗号鍵３４１ｂを割り当て、１ｃに対応するＩＰアドレス３１ｃにデータ種別３２６ａ、暗号鍵３４１ａを割り当てている。

【００５５】また、端末１ｄ、１ｅに対応するＩＰアドレス３１ｄ、３１ｅに、それぞれデータ種別３２６ｂと暗号鍵３４１ｂを割り当てている。以下同様に端末１ｂ～１ｅに対応する暗号装置３ｂ～３ｅの暗号化情報テーブル２ｂ～２ｅには図４に示すＩＰアドレス、データ種別、暗号鍵を割り当てている。

【００５６】次に、図５および図６を用いて端末１ａ、１ｂ間を例にデータ送受信の動作を説明する。通信に先立ち暗号装置３ａにおいて、通信相手のＩＰアドレス（３１ｂ）、データ種別、暗号鍵を組にして図４の暗号化情報テーブル２ａに登録する。また、暗号装置３ｂにおいて、通信相手のＩＰアドレス（３１ａ）、データ種別、暗号鍵を組にして暗号化情報テーブル２ｂに登録する。登録方法は図１に示す保守端末６１を操作することにより、暗号装置３ａ、３ｂの装置機能設定部１４を介して暗号処理部１３が暗号化情報テーブル２ａ、２ｂに登録情報、即ち通信相手のＩＰアドレス（３１ｂ）、データ種別、暗号鍵を組にして記憶する。

【００５７】次に、図５によりデータ送信の動作を自端末１ａから相手端末１ｂ宛を例に説明する。自端末１ａは、図４のＩＰパケットの送信元ＩＰアドレス部４０１に自端末１ａのＩＰアドレス３１ａを設定し、宛先ＩＰアドレス部４０２に送信相手の端末１ｂのＩＰアドレス３１ｂを設定し、データ種別部４３１にデータ種別（例えば３２６ａ）を設定し、ＩＰパケット４４５を暗号装置３ａへ送る。ステップ４５２で暗号装置３ａが端末１ａからＩＰパケット４４５を受け取る。ステップ４５３で、図１の暗号装置３ａの端末側送受信部１５は、前記のＩＰパケット４４５を受け取りデータ格納メモリ１７に書き込み、中央処理装置１１にＩＰパケット４４５を受け取ったことを伝える。ステップ４５４に進み、中央処理装置１１は、暗号処理部１３に対しＩＰパケット４４５を受け取ったことを伝え、暗号化を指示する。

【００５８】そして、ステップ４５６に進み、暗号処理部１３は、データ格納メモリ１７からＩＰパケット４４５を読み取り、宛先ＩＰアドレスとデータ種別の組と一致するものが図４の暗号化情報テーブル２ａ内にあるかサーチし、一致するものがない場合は、暗号化せずステップ４５８に進む。一致するものがあれば、ステップ４５７に進み、そのＩＰアドレスとデータ種別の組で登録しておいた暗号鍵でＩＰパケット４４５のＴＣＰデータ部４４２を暗号化し、ステップ４５８に進む。ステップ４５８で、処理が終了したことを中央処理装置１１に伝え、ステップ４５９に進む。ステップ４５９で中央処理装置１１は、ＩＰパケット４４５を通信網９１ａに送信するように網側送受信部１６に指示する。そして、ステップ４６０で網側送受信部１６は、データ格納メモリ１７からＩＰパケット４４５を読み取り、通信網９１ａへ送る。

【００５９】以上のように、送信するＩＰパケット４４５内の宛先ＩＰアドレスとデータ種別の組と一致するものが暗号化情報テーブル２内にあれば、その暗号化情報テーブル２がＩＰアドレスとデータ種別の組にして登録しておいた暗号鍵で、ＩＰパケット４４５のＴＣＰデータ部４４２を暗号化し送信する。同じものがなければ、暗号化せずＩＰパケット４４５を送信する。

【００６０】次に、図６により、データ受信の動作を相手端末１ａから自端末１ｂ宛を例に説明する。ステップ４６３で自端末１ｂの暗号装置３ｂは、自端末宛のＩＰパケット４４５を通信網９１ａから受け取る。ステップ４６４で暗号装置３ｂの網側送受信部１６は、前記のＩＰパケット４４５を受信しデータ格納メモリ１７に書き込み、中央処理装置１１に対してＩＰパケット４４５の受信を伝える。ステップ４６５で中央処理装置１１は、暗号処理部１３に対しＩＰパケット４４５の受信を伝え、復号を指示する。

【００６１】ステップ４６７で暗号処理部１３は、データ格納メモリ１７からＩＰパケット４４５を読み取り、ＩＰパケット４４５内の送信元ＩＰアドレスとデータ種

別の組と一致するものが暗号化情報テーブル２ｂ内にあるかサーチし、一致するものがない場合は、復号せずステップ４６９に進む。一致するものがあれば、ステップ４６８に進み、そのＩＰアドレスとデータ種別の組で登録しておいた暗号鍵でＩＰパケット４４５のＴＣＰデータ部４４２を復号する。そして、ステップ４６９で、処理が終了したことを中央処理装置１１に伝えステップ４７０に進む。ステップ４７０で中央処理装置１１は、ＩＰパケット４４５を自端末１ｂに送信するように端末側送受信部１５に指示する。ステップ４７１で端末側送受信部１５は、データ格納メモリ１７からＩＰパケット４４５を読み取り自端末１ｂへ渡す。自端末１ｂは、暗号装置３ｂからＩＰパケット４４５を受け取る。

【００６２】以上のように、暗号装置３は受信したＩＰパケット４４５内の送信元ＩＰアドレスとデータ種別の組と一致するものが暗号化情報テーブル２内にあれば、そのＩＰアドレスとデータ種別の組にして暗号化情報テーブル２に登録しておいた暗号鍵でＩＰパケット４４５のＴＣＰデータ部４４２を復号し、ＩＰパケット４４５を端末に渡す。同じものがなければ、復号せずＩＰパケット４４５を端末に渡す。また、逆に端末１ｂから端末１ａにデータを送る動作は上記の説明で端末１ａと端末１ｂを置き換えたものと同様である。

【００６３】次に、端末１ａと端末１ｂとの間で異なるデータ種別３２６ａと３２６ｂで暗号通信する例と、登録していないデータ種別３２６ｆを用いて通信する例を説明する。図４に示すように、あらかじめ暗号装置３ａの暗号化情報テーブル２ａに通信相手のＩＰアドレス３１ｂとデータ種別３２６ａと暗号鍵３４１ａの組と、通信相手のＩＰアドレス３１ｂとデータ種別３２６ｂと暗号鍵３４１ｂの組と、を登録しておく。また、暗号装置３ｂの暗号化情報テーブル２ｂに、通信相手のＩＰアドレス３１ａとデータ種別３２６ａと暗号鍵３４１ａの組と、通信相手のＩＰアドレス３１ａとデータ種別３２６ｂと暗号鍵３４１ｂの組と、を登録しておく。次に、端末１ａがデータ種別３２６ａで端末１ｂにデータを送信する例を説明する。

【００６４】自端末１ａは送信元ＩＰアドレスに３１ａを、宛先ＩＰアドレスに３１ｂを、データ種別に３２６ａを設定し、相手端末１ｂ宛のＩＰパケット４４５を編集して、暗号装置３ａに渡す。暗号装置３ａは宛先ＩＰアドレス３１ｂとデータ種別３２６ａが暗号化情報テーブル２ａにあるか調べ、あるので、関連する暗号鍵３４１ａで暗号化し通信網９１ａに送出する。端末１ｂの暗号装置３ｂは通信網９１ａから自端末宛ＩＰパケット４４５を受信し、送信元ＩＰアドレスとデータ種別３２６ａの組と同じものがあるか調べ、暗号化情報テーブル２ｂにあるので、暗号装置３ｂはＩＰアドレスとデータ種別と組をなす暗号鍵３４１ａで復号し、端末１ｂに渡す。

【００６５】次に、端末１ａが端末１ｂからデータを受信する例を説明する。端末１ｂは送信元ＩＰアドレス３１ｂ、宛先ＩＰアドレス３１ａ、データ種別３２６ａのＩＰパケット４４５を編集して、暗号装置３ｂに渡す。暗号装置３ｂは宛先ＩＰアドレス３１ａとデータ種別３２６ａの組と同じものが暗号化情報テーブル２ｂにあるか調べ、あるので、暗号装置３ｂはＩＰアドレスとデータ種別の組に対応する暗号鍵３４１ａで暗号化し通信網９１ａに送出する。端末１ａの暗号装置３ａは通信網９１ａから自端末宛ＩＰパケット４４５を受信し、送信元ＩＰアドレスとデータ種別の組と一致するものが暗号化情報テーブル２ａにあるか調べ、あるので暗号装置３ａはＩＰアドレスとデータ種別と組をなす暗号鍵３４１ａで復号し、端末１ａに渡す。

【００６６】次に、端末１ａがデータ種別３２６ｂで端末１ｂにデータを送信する例は、上記で用いたデータ種別３２６ａを３２６ｂに置き換え同様の動作で通信ができる。ただし、暗号化・復号はデータ種別３２６ｂに対応して登録した暗号鍵３４１ｂを使用する。以上のように、同じ端末相互にデータ種別に応じ、異なる暗号鍵で暗号通信ができる。

【００６７】次に、端末１ａが未登録のデータ種別３２６ｆで端末１ｂにデータを送信する例を説明する。自端末１ａは送信元ＩＰアドレス３１ａ、宛先ＩＰアドレス３１ｂ、データ種別３２６ｆのＩＰパケット４４５を編集して、暗号装置３ａに渡す。暗号装置３ａは宛先ＩＰアドレス３１ｂとデータ種別３２６ｆの組と一致するものが暗号化情報テーブル２ａにあるか調べ、ないので、暗号化せずに通信網９１ａに送出する。端末１ｂの暗号装置３ｂは通信網９１ａから自端末宛ＩＰパケット４４５を受信し、送信元ＩＰアドレスとデータ種別の組と一致するものが暗号化情報テーブル２ｂにあるか調べ、ないので暗号装置３ｂは復号せず端末１ｂに渡す。

【００６８】次に、端末１ａが端末１ｂからデータを受信する例を説明する。端末１ｂは送信元ＩＰアドレス３１ｂ、宛先ＩＰアドレス３１ａ、データ種別３２６ｆのＩＰパケット４４５を編集して、暗号装置３ｂに渡す。暗号装置３ｂは宛先ＩＰアドレス３１ａとデータ種別３２６ｆの組と一致するものが暗号化情報テーブル２ｂにあるか調べ、ないので、暗号装置３ｂは暗号化せず通信網９１ａに送出する。端末１ａの暗号装置３ａは通信網９１ａから自端末宛ＩＰパケット４４５を受信し、送信元ＩＰアドレスとデータ種別の組と一致するものが暗号化情報テーブル２ａにあるか調べ、ないので暗号装置３ａは復号せず端末１ａに渡す。

【００６９】以上、２つの端末間で、データ種別によって異なる暗号で通信ができるので暗号強度が増す。また、暗号通信の必要がなければ未登録のデータ種別を用いることにより暗号化せずに通信することもでき、暗号化・復号に掛かる無駄な遅延時間をなくすことができ

る。

【００７０】次に、端末１ａから、暗号装置３ａが接続されていない端末１ｆとの通信について説明する。あらかじめ暗号化情報テーブル２ａから端末１ｆのＩＰアドレス３１ｆを除いておく。図５および図６で説明したように、端末１ａが送信元ＩＰアドレス３１ａ、宛先ＩＰアドレス３１ｆのＩＰパケット４４５を編集して暗号装置３ａに渡す。暗号装置３ａは宛先ＩＰアドレス３１ｆが暗号化情報テーブル２ａにあるか調べ、登録していないので一致するものがなく暗号装置３ａは暗号化せず送信する。次は逆に端末１ｆからの端末１ａ宛のＩＰパケット４４５を受信した暗号装置３ａは暗号化情報テーブル２ａに送信元ＩＰアドレス３１ｆがないので復号せずに受信したＩＰパケット４４５を端末１ａに渡す。従って、暗号装置３を介して通信網９１ａに接続された端末１と暗号装置３を介さず直接通信網９１ａに接続された端末１間でも暗号化せずに通信できる。

【００７１】図４のようにＩＰアドレス、データ種別、暗号鍵の組が登録されている状態で図２の通信網構成なら、上記の動作原理から端末１ａ、１ｂ、１ｃ、は同じデータ種別３２６ａを使って相互に暗号通信ができ、端末１ａ、１ｂ、１ｄ、１ｅは同じデータ種別３２６ｂを使って相互に暗号通信ができる。従って、図２に示す通信閉域１８３ａ、１８３ｂのように端末相互に同一データ種別を用いた暗号通信の通信閉域を構成できる。また、端末１ｄ、１ｅと端末１ｃは通信相手のＩＰアドレスが登録されていないので、相互に暗号化せずに通信できる。また、暗号装置３が接続されていない端末１ｆ～１ｈは他の端末１ａ～１ｈと暗号化せずに通信できる。

【００７２】なお、データ種別を同じにして暗号鍵を共有する例を示したが、データ種別は端末におけるデータ送受信の要求元のアプリケーションプログラムを識別するものであってもよい。また、上記実施例ではＴＣＰ／ＩＰの通信手順の場合について説明したが、ＩＰＸ（Internet Packet Exchange）やその他の通信手順であってもよく、上記実施例と同様の効果を奏する。また、端末１と暗号装置３は１対１に接続している例を示したが暗号装置３に複数台の端末１を接続しても同様の効果を奏する。

【００７３】暗号装置３に複数の端末１を接続する方法として、受信のときはＩＰパケット４４５の宛先ＩＰアドレス部４０２にもとずいて、送信のときは送信元ＩＰアドレス部４０１にもとずいて暗号装置３に収容される端末１を識別することにより暗号通信が可能である。たとえば、あらかじめ宛先アドレス、送信元アドレスと暗号鍵の組み合わせを暗号化情報テーブル２に登録しておく。ただし、宛先アドレスまたは送信元アドレスには暗号装置３に収容される端末１のアドレスを登録する。

【００７４】端末１からＩＰパケット４４５を受信したとき、そのＩＰパケット４４５の宛先アドレスと送信元アドレスが暗号化情報テーブル２に登録されていれば、宛先アドレスと送信元アドレスに関連して登録されている暗号鍵でＩＰパケット４４５のＩＰデータ部４１２を暗号化し、通信網９１ａに送信する。逆に、通信網９１ａから受信したＩＰパケット４４５の宛先アドレスと送信元アドレスが暗号化情報テーブル２に登録されていれば、宛先アドレスと送信元アドレスに関連して登録されている暗号鍵でＩＰパケット４４５のＩＰデータ部４１２を復号し、宛先アドレスの示す端末１へ受信したＩＰパケット４４５を渡す。

【００７５】また、データ種別により使用する暗号鍵を変えるには、あらかじめ宛先アドレス、送信元アドレス、データ種別および暗号鍵の組み合わせを暗号化情報テーブル２に登録しておく。以下同様に、端末１からＩＰパケット４４５を受信したとき、そのＩＰパケット４４５の宛先アドレス、送信元アドレスおよびデータ種別が暗号化情報テーブル２に登録されていれば、宛先アドレス、送信元アドレスおよびデータ種別に関連して登録されている暗号鍵でＩＰパケット４４５のＴＣＰデータ部４４２を暗号化し、通信網９１ａに送信する。逆に、通信網９１ａから受信したＩＰパケット４４５の宛先アドレス、送信元アドレスおよびデータ種別が暗号化情報テーブル２に登録されていれば、宛先アドレス、送信元アドレスおよびデータ種別に関連して登録されている暗号鍵でＩＰパケット４４５のＴＣＰデータ部４４２を復号し、宛先アドレスの示す端末１へ受信したＩＰパケット４４５を渡す。以上により暗号装置３に複数の端末１を接続することができ、データ種別によって暗号鍵を変えることができる。

【００７６】次に、上記例では、通信相手のＩＰアドレスをもとに使用する暗号鍵を決めていたが、ＩＰアドレスの上位ビットが同一の端末でネットワークまたはサブネットワークを構成し、そのネットワーク内の各端末が同じ暗号鍵を用いて他の端末と暗号通信する場合は、ＩＰアドレスのネットワークを識別する上位桁をもとに暗号鍵を決めることもできる。ここで、図１８はＩＰアドレス４０３の構成を示す図で、４０４はＩＰアドレスの上位桁で、ネットワークまたはサブネットワークのアドレスを示す。４０５はそのネットワーク内の端末識別子を示す。

【００７７】そして、上記実施例の図４の暗号化情報テーブルのＩＰアドレスとデータ種別の組で一致するものをサーチする場合、ＩＰアドレス一致の判定の代わりにネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。即ち、図５のステップ４５６および図６のステップ４６７においてＩＰアドレス一致の判定の代わりにネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。他は上記実施例と同様である。以上のようにネットワーク対応に暗号鍵を割り当てれば、同じネットワークに属す

る端末には同じネットワークアドレスを登録すればよいので、端末ごと異なるＩＰアドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【００７８】実施例２．本実施例は、複数の暗号鍵を用いて暗号強度の強い通信を行なおうとするものである。図１は暗号装置の構成を示し、図２は通信システムの構成例を示し、図３は送受信データの構成を示すが、実施例１と同一で説明を省略する。図７は、暗号装置３対応に設けた暗号化情報テーブル２の内容を例示するものであり、実施例１の図４とは異なる。図７において、２ａ～２ｅは暗号装置３ａ～３ｅ対応に設けた暗号化情報テーブル２で、通信相手のＩＰアドレス、暗号鍵有効情報、第１暗号鍵、第２暗号鍵を一組として関連ずけて記憶する。３１ａ～３１ｅはそれぞれ端末１ａ～１ｅのＩＰアドレスである。

【００７９】また、３４１ｃおよび３４１ｄは暗号鍵である。そして、３２７ａ、３２７ｂ、３２７ｃは暗号鍵有効情報に設定する値で、複数の暗号鍵を使用するか否かと、使用するなら鍵を使う順番を指定するものである。どの鍵を使うかは暗号化情報テーブル２の指定による。即ち、図７の例で、暗号鍵有効情報の値が３２７ａなら第１暗号鍵と第２暗号鍵が有効で、暗号化には第１暗号鍵の次に第２暗号鍵を用いることを、復号には逆に第２暗号鍵の次に第１暗号鍵を用いることを意味する。暗号鍵有効情報の値が３２７ｂなら第１暗号鍵のみが有効で、暗号化・復号に第１暗号鍵を用いることを意味し、暗号鍵有効情報の値が３２７ｃなら第２の暗号鍵のみが有効で、暗号化・復号に第２暗号鍵を用いることを意味する。

【００８０】次に暗号装置３の送信動作について図８を用いて説明する。本図は実施例の図５と比較し、ステップ４５６、４５７をステップ４５５、４７３～４７７に置き換えたもので、ステップ４５５で送信ＩＰパケット４４５の宛先ＩＰアドレスに一致するものが図７の暗号化情報テーブル２内にあるかサーチして、一致するものがない場合は、復号せずステップ４５８に進む。一致するものがあれば、ステップ４７３に進み、その宛先ＩＰアドレスと組をなす暗号鍵有効情報の値に従い、値が３２７ｂなら、ステップ４７４に進み第１暗号鍵を用いてＩＰデータ部４１２のデータを暗号化し、値が３２７ｃならステップ４７５に進み第２暗号鍵を用いてＩＰデータ部４１２のデータを暗号化し、値が３２７ａならステップ４７６に進み、第１暗号鍵を用いてＩＰデータ部４１２のデータを暗号化し、ステップ４７７で、暗号化したＩＰデータ部４１２のデータをさらに第２暗号鍵を用いて暗号化し、ステップ４５８に進む。他の動作は実施例１の図５と同じで説明を省略する。

【００８１】また、受信動作について図９を用いて説明する。本図は実施例の図６と比較し、ステップ４６７、４６８をステップ４６６、４７８～４８２に置き換えたもので、ステップ４６６で受信したＩＰパケット４４５内の送信元ＩＰアドレスと同じものが暗号化情報テーブル２ｂ内にあるかサーチし、一致するものがなければ復号せずステップ４６９に進む。一致するものがあれば、ステップ４７８に進み、そのＩＰアドレスと組をなす暗号鍵有効情報の値に従い、その暗号鍵有効情報の値が３２７ｂなら、ステップ４７９に進み第一暗号鍵を用いてＩＰデータ部４１２のデータを復号し、値が３２７ｃならステップ４８０に進み第２暗号鍵を用いてＩＰデータ部４１２のデータを復号し、値が３２７ａならステップ４８１に進み、第２暗号鍵を用いてＩＰデータ部４１２のデータを復号し、ステップ４８２で、復号したＩＰデータ部４１２のデータをさらに第１暗号鍵を用いて、復号を行う。そして、ステップ４６９に進む。他の動作は実施例１の図６と同じで説明を省略する。

【００８２】第１暗号鍵と第２暗号鍵を使って端末１ａから端末１ｂへ送信する例を説明する。通信に先立ち、第１暗号鍵と第２暗号鍵を使って暗号通信するよう暗号鍵有効情報に３２７ａを登録する。即ち、図７のようにあらかじめ暗号化情報テーブル２ａのＩＰアドレスに３１ｂ、暗号鍵有効情報に３２７ａ、第１暗号鍵に３４１ｃ、第２暗号鍵に３４１ｄを登録し、暗号化情報テーブル２ｂのＩＰアドレスに３１ａ、暗号鍵有効情報に３２７ａ、第１暗号鍵に３４１ｃ、第２暗号鍵に３４１ｄを登録しておく。次に、端末１ａが送信元ＩＰアドレス３１ａ、宛先ＩＰアドレス３１ｂのＩＰパケット４４５を編集し、暗号装置３ａに渡す。暗号装置３ａは宛先ＩＰアドレス３１ｂに一致するものが暗号化情報テーブル２ａにあるかサーチし、あればＩＰアドレス３１ｂと組をなす暗号鍵有効情報の値３２７ａに従い第１暗号鍵でＩＰデータ部４１２のデータを暗号化し、さらに第２暗号鍵で暗号化し、端末１ｂ宛送信する。

【００８３】次に、端末１ｂの暗号装置３ｄは通信網９１ａから宛先ＩＰアドレス３１ｂのＩＰパケット４４５を受信し、送信元ＩＰアドレス３１ａに一致するものが暗号化情報テーブル１ｂにあるか調べ、あるので、送信元ＩＰアドレス３１ａと組をなす暗号鍵有効情報の値３２７ａに従い、第２暗号鍵でＩＰデータ部４１２のデータを復号した後、さらに第１暗号鍵で復号し端末１ｂに渡す。以下、第１暗号鍵のみを用いるときは暗号鍵有効情報に３２７ｂを、第２暗号鍵のみを用いるときは暗号鍵有効情報に３２７ｃを登録しておき、暗号化しないときはなにも登録しておかなければよい。

【００８４】以上、本実施例では２つまでの鍵を用いた例を示したが２つ以上の複数鍵を用いてもよい。複数回暗号化すると暗号強度は増すが暗号化の演算量が増え暗号化・復号に時間が掛かるが、通信相手によって暗号化の回数と各回に用いる暗号鍵を選ぶことにより暗号強度を変えることができる。図７のようにＩＰアドレス、暗号鍵有効情報、第１暗号鍵、第２暗号鍵の組が登録され

ている状態で、図２の通信網構成なら、上記の動作原理から端末１ａ、１ｂ、１ｃは第１暗号鍵３４１ｃを使って暗号通信ができ、端末１ａ、１ｂ、１ｄ、１ｅは第２暗号鍵３４１ｄを使って相互に暗号通信ができる。従って、端末相互に同一鍵を用いた暗号通信の通信閉域を構成できる。また、端末１ｄ、１ｅと端末１ｃは通信相手のＩＰアドレスが登録されていないので相互に暗号化せずに通信できる。また、暗号装置３が接続されていない端末１ｆ～１ｈは他の端末１ａ～１ｈと暗号化せずに通信できる。

【００８５】また、本実施例は端末１のＩＰアドレス対応に暗号鍵を割り当てているが、実施例１のようにＩＰアドレスとデータ種別の組に対応して本実施例の暗号鍵を割り当て、暗号鍵に秘密鍵有効情報、第１暗号鍵、第２暗号鍵を用いて暗号強度に応じた暗号化を行うこともでき、２つ以上の複数鍵を用いて複数回暗号化・復号してもよい。また、暗号装置３に複数の端末１を接続する例においても、宛先アドレアス、送信元アドレスの組、および宛先アドレアス、送信元アドレスとデータ種別の組に対応して上記のように本実施例の暗号鍵を割り当ててもよい。なお、上記実施例では、暗号化・復号する送受信データの範囲をＩＰデータ部４１２に適用したが、ＴＣＰデータ部４４２に適用してもよい。また、上記実施例ではＴＣＰ／ＩＰの通信手順の場合について説明したが、ＩＰＸ（Internet Packet Exchange）やその他の通信手順であってもよく、上記実施例と同様の効果を奏する。

【００８６】また、端末１と暗号装置３は１対１に接続している例を示したが暗号装置３に複数台の端末１を接続しても同様の効果を奏する。次に、上記例では、通信相手のＩＰアドレスをもとに使用する暗号鍵を決めていたが、ＩＰアドレスの上位ビットが同一の端末でネットワークまたはサブネットワークを構成し、そのネットワーク内の各端末が同じ暗号鍵を用いて他の端末と暗号通信する場合は、ＩＰアドレスのネットワークを識別する上位桁をもとに暗号鍵を決めることもできる。

【００８７】上記実施例の図７の暗号化情報テーブルのＩＰアドレスと一致するものをサーチする場合、ＩＰアドレス一致の判定の代わりに図１８のネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。即ち、送信の場合は図８のステップ４５５および受信の場合は図９のステップ４６６においてＩＰアドレス一致の判定の代わりにネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。他は上記実施例と同様である。このようにネットワーク対応に暗号鍵を割り当てれば、同じネットワークに属する端末には同じネットワークアドレスを登録すればよいので、端末ごと異なるＩＰアドレスの下位ビットを登録しなくてもよく、操作労力を軽減できる。

【００８８】実施例３．相互に暗号通信する必要のない安全域のネットワークに属する端末が、暗号通信を必要とする危険域内の端末と通信する際、危険域内は暗号通信できるようにするものである。図１は暗号装置の構成を示し、図３は送受信データの構成を示すが、実施例１と同一で説明を省略する。図１０は、第１通信網と第２通信網の間に暗号装置３ｍを設けた構成を示す図であり、図において、１６は第１網側送受信部、１８は第２網側送受信部、３ｍは暗号装置、９１ａは危険域の第１通信網、９１ｂは安全域の第２通信網で、他は図１と同じで説明を省略する。

【００８９】図１１は暗号通信システムの構成例を示す図であり、図においては、９１ａは暗号通信の必要のある危険域の第１の通信網、９１ｂは暗号通信の必要のない安全域の第２の通信網、１ａ～１ｈは第１の通信網９１ａに属する端末、１ｉ～１ｌは第２の通信網９１ｂに属する端末、３ａ～３ｅは各々端末１ａ～１ｅに対応して設けた暗号装置、３ｍは第１通信網９１ａと第２通信網９１ｂ間の暗号通信の中継を行う暗号装置である。図１２は、暗号装置３ごとに設けた暗号化情報テーブル２の内容を例示するものであり、図において、２ａ、２ｂ、２ｅは各々暗号装置３ａ、３ｂ、３ｅ対応に設けた暗号化情報テーブルで、内容は異なるが実施例２の図７に示す暗号化情報テーブル２と同じ構成である。

【００９０】２ｍは暗号装置３ｍが暗号化・復号のために用いる暗号化情報テーブルで、第１の通信網側ＩＰアドレス、第２の通信網側ＩＰアドレス、暗号鍵有効情報、第１暗号鍵、第２暗号鍵を一組として関連ずけて記憶する。３１ａ、３１ｂ、３１ｅは端末１ａ、１ｂ、１ｅのＩＰアドレス、３１ｉ、３１ｊ、３１ｋは端末１ｉ、１ｊ、１ｋのＩＰアドレスである。また、３４１ｅおよび３４１ｆは暗号化・復号で用いる暗号鍵、３２７ｂは実施例２で説明した暗号鍵有効情報で、第１暗号鍵のみが暗号化・復号に有効であることを示す。

【００９１】通信に先立ち暗号装置３ａにおいて、通信相手のＩＰアドレス（３１ｉ）、暗号鍵有効情報、第１暗号鍵、第２暗号鍵を組にして図１２の暗号化情報テーブル２ａに登録する。また、暗号装置３ｍにおいて、第１網側ＩＰアドレス（３１ａ）、第２網側ＩＰアドレス（３１ｉ）、暗号鍵有効情報、第１暗号鍵、第２暗号鍵を組にして暗号化情報テーブル２ｍに登録する。

【００９２】図１３は第１通信網９１ａから第２通信網９１ｂに中継する例を示す。この図により、データ送信の動作を相手端末１ａから自端末１ｉ宛を例に説明する。端末１ａは送信元ＩＰアドレス３１ａ宛先ＩＰアドレス３１ｉのＩＰパケット４４５を編集し、暗号装置３ａに渡す。暗号装置３ａは実施例２の図８と同様に第１通信網９１ａへ暗号化したＩＰパケット４４５を送信する。ステップ４６３で暗号装置３ｍは、宛先ＩＰアドレス３１ｉのＩＰパケット４４５を第１通信網９１ａから受信する。

【００９３】そしてステップ４６４に進み、図１０の暗号装置３ｍの第１網側送受信部１６は、前記のＩＰパケット４４５を受信しデータ格納メモリ１７に書き込み、中央処理装置１１に対してＩＰパケット４４５の受信を伝える。ステップ４６５で中央処理装置１１は、暗号処理部１３に対しＩＰパケット４４５の受信を伝え、復号を指示する。ステップ４６６で、暗号処理部１３は、データ格納メモリ１７からＩＰパケット４４５を読み取り、宛先ＩＰアドレス３１ｉと送信元ＩＰアドレス３１ａの組と同じものが暗号化情報テーブル２ｍ内にあるかサーチする。一致するものがなければステップ４６９に進む。

【００９４】一致するものがあればステップ４７８に進み、ＩＰアドレス３１ａとＩＰアドレス３１ｉと組をなす暗号鍵有効情報の値に従い、その値が３２７ｂなら、ステップ４７９に進み第１暗号鍵を用いてＩＰデータ部４１２のデータを復号し、暗号鍵有効情報の値が３２７ｃならステップ４８０に進み第２暗号鍵を用いてＩＰデータ部４１２のデータを復号し、暗号鍵有効情報の値が３２７ａならステップ４８１に進み、第２暗号鍵を用いてＩＰデータ部４１２のデータを復号し、ステップ４８２で、復号したＩＰデータ部４１２のデータをさらに第１暗号鍵を用いて、復号を行う。そして、ステップ４６９で処理が終了したことを中央処理装置１１に伝える。ステップ４７０で、中央処理装置１１は、ＩＰパケット４４５を第２通信網９１ｂに送信するように第２網側送受信部１８に指示する。そしてステップ４７１で第２網側送受信部１８は、データ格納メモリ１７からＩＰパケット４４５を読み取り、第２通信網９１ｂへ送る。端末１ｉは、第２通信網９１ｂから宛先ＩＰアドレス３１ｉの自端末宛ＩＰパケット４４５を受け取る。

【００９５】次に、図１４は第２通信網９１ｂから第１通信網９１ａにデータを中継する例を示す。図１４により、端末１ａが端末１ｉからデータを受信する例について説明する。端末１ｉは、送信元ＩＰアドレス３１ｉで宛先ＩＰアドレス３１ａのＩＰパケット４４５を編集し第２通信網９１ｂへ送る。暗号装置３ｍは、ステップ４５２で宛先ＩＰアドレス３１ａのＩＰパケット４４５を第２通信網９１ｂから受け取る。ステップ４５３で、暗号装置３ｍの第２網側送受信部１８は、前記のＩＰパケット４４５を受信しデータ格納メモリ１７に書き込み、中央処理装置１１に対してＩＰパケット４４５の受信を伝える。ステップ４５４で、中央処理装置１１は、暗号処理部１３に対しＩＰパケット４４５の受信を伝え、暗号化を指示する。

【００９６】ステップ４８４で暗号処理部１３は、データ格納メモリ１７からＩＰパケット４４５を読み取り、宛先ＩＰアドレス３１ａと送信元ＩＰアドレス３１ｉと一致するものが暗号化情報テーブル２ｍ内あるかサーチし、一致するものがなければステップ４５８に進む。一致するものがあれば、ステップ４７３に進み、ＩＰアドレス３１ａとＩＰアドレス３１ｉと組をなす暗号鍵有効情報の値に従い、その値が３２７ｂなら、ステップ４７４に進み第１暗号鍵を用いてＩＰデータ部４１２のデータを暗号化し、暗号鍵有効情報の値が３２７ｃならステップ４７５に進み第２暗号鍵を用いてＩＰデータ部４１２のデータを暗号化し、暗号鍵有効情報の値が３２７ａならステップ４７６に進み、第１の暗号鍵を用いてＩＰデータ部４１２のデータを暗号化し、ステップ４７７で、暗号化したＩＰデータ部４１２のデータをさらに第２の暗号鍵を用いて、暗号化を行う。そして、ステップ４５８に進み、処理が終了したことを中央処理装置１１に伝える。ステップ４５９で中央処理装置１１は、ＩＰパケット４４５を第１通信網９１ａに送信するように第１網側送受信部１６に指示する。

【００９７】ステップ４６０で第１網側送受信部１６は、データ格納メモリ１７からＩＰパケット４４５を読み取り、第１通信網９１ａへ送る。暗号装置３ａは、実施例２の図９と同様に第１通信網９１ａからＩＰパケット４４５を受け取り、ＩＰデータ部４１２を復号して端末１ａへ渡す。

【００９８】以上により、第１通信網９１ａ（危険域）からのＩＰパケット４４５を復号し第２通信網９１ｂ（安全域）へ中継し、逆に第２通信網９１ｂ（安全域）の端末からＩＰパケット４４５を暗号化し第１通信網９１ａ（危険域）に中継できる。従って、安全域に属する複数の端末１対応に暗号装置３を設ける必要はなく、さらに暗号登録する必要もなく鍵の配布労力が省ける。図１２のように暗号化情報テーブル２が登録されている状態で、図１１の通信網構成なら、上記の動作原理から端末１ａ、１ｂと端末１ｉ間は暗号鍵３４１ｅを用いて相互に危険域で暗号通信ができ、端末１ｅ、１ｊ、１ｋ間は暗号鍵３４１ｆを用いて相互に危険域で暗号通信ができる。従って、端末１ａ、１ｂ、１ｉは、共通の暗号鍵３４１ｅを用いた暗号通信の通信閉域を、端末１ｅ、１ｊ、１ｋは、共通の暗号鍵３４１ｆを用いた暗号通信の通信閉域を構成できる。

【００９９】また、上記実施例では、暗号化・復号する送受信データの範囲をＩＰデータ部４１２に適用したが、ＴＣＰデータ部４４２に適用してもよい。そして、上記実施例ではＴＣＰ／ＩＰの通信手順の場合について説明したが、ＩＰＸ（Internet Packet Exchange）やその他の通信手順であってもよく、上記実施例と同様の効果を奏する。さらに、上記例では暗号鍵として一つの鍵を用いる例を示したが、実施例２のように暗号鍵に秘密鍵有効情報、第１暗号鍵、第２暗号鍵を用いて暗号強度に応じた暗号化を行うこともでき、２つ以上の複数鍵を用いて複数回暗号化・復号してもよい。

【０１００】またＩＰアドレスをもとに使用する暗号鍵を決めていたが、実施例１のようにＩＰアドレスとデー

タ種別に対応して本実施例の暗号鍵を割り当ててもよい
次に、上記例では、通信相手のＩＰアドレスをもとに使用する暗号鍵を決めていたが、ＩＰアドレスの上位ビットが同一の端末でネットワークまたはサブネットワークを構成し、そのネットワーク内の各端末が同じ暗号鍵を用いて他の端末と暗号通信する場合は、ＩＰアドレスのネットワークを識別する上位桁をもとに暗号鍵を決めることもできる。

【０１０１】上記実施例の図１２の暗号化情報テーブル２ｍのＩＰアドレスと一致するものをサーチする場合、ＩＰアドレス一致の判定の代わりに、図１８のネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。即ち、第２通信網内で同じ暗号鍵を用いる場合は図１３のステップ４６６の宛先ＩＰアドレスおよび図１４のステップ４８４の送信元ＩＰアドレス一致の判定の代わりに、図１８のネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。また、第１通信網内で同じ暗号鍵を用いる場合、図１３のステップ４６６の送信元ＩＰアドレスおよび図１４のステップ４８４の宛先ＩＰアドレス一致の判定の代わりに図１８のネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。
他は上記実施例と同様である。以上のようにネットワーク対応に暗号鍵を割り当てれば、同じネットワークに属する端末には同じネットワークアドレスを登録すればよいので、端末ごと異なるＩＰアドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【０１０２】実施例４．本実施例は送信・受信に異なる暗号鍵を使えるようにしようとするものである。図１は暗号装置の構成を示し、図２は、暗号通信システムの構成例を示し、図３は送受信データの構成を示すが、実施例１と同一で説明を省略する。図１５は暗号化情報テーブル２の内容を例示するものであり、実施例１の図４とは異なる。図において、２ａ～２ｅは暗号装置３ａ～３ｅ対応に設けた暗号化情報テーブルで、通信相手ＩＰアドレスと送信用暗号鍵、および受信用暗号鍵とを関連ずけて記憶する。そして、送信・受信しようとするＩＰパケット４４５の宛先ＩＰアドレス・送信元ＩＰアドレスが暗号化情報テーブル２の通信相手ＩＰアドレスに一致するものがあるか調べ、あるなら、その組に対応する送信用・受信用暗号鍵を用いて暗号化・復号し、一致するものがなければ、暗号化・復号せずにＩＰパケット４４５を送信・受信することを意味する。

【０１０３】例えば、図１５の暗号装置３ａの暗号化情報テーブル２ａの暗号鍵３４１ｇはＩＰアドレス３１ａからＩＰアドレス３１ｂ宛の暗号化で用いる送信用暗号鍵で、暗号鍵３４１ｈは逆に端末１ｂから端末１ａ宛で復号に用いる受信用暗号鍵である。一方暗号装置３ｂの暗号化情報テーブル２ｂの暗号鍵３４１ｈはＩＰアドレス３１ｂからＩＰアドレス３１ａ宛のＩＰパケット４４５を暗号化するのに用いる送信用暗号鍵で、暗号鍵３４１ｇは逆に端末１ａから端末１ｂ宛でＩＰパケット４４５を復号するのに用いる受信用暗号鍵である。他の暗号鍵３４１ｉ～３４１ｎも同様に送受別の鍵となるよう構成している。なお、３１ａ～３１ｅは端末１ａ～１ｅのＩＰアドレスである。

【０１０４】次に暗号装置３の送信動作について図１６を用いて説明する。本図は実施例１の図５と比較し、ステップ４５６、４５７をステップ４９５、４９６に置き換えてたもので、ステップ４９５で送信ＩＰパケット４４５の宛先ＩＰアドレスと暗号化情報テーブル２内の通信相手ＩＰアドレスとを比較し一致する通信相手ＩＰアドレスをサーチして、一致するものがない場合は、暗号化せずステップ４５８に進む。一致するものがあれば、ステップ４９６に進み、その通信相手のＩＰアドレスに対応して登録しておいた送信用暗号鍵でＩＰパケット４４５のＩＰデータ部４１２を暗号化し、ステップ４５８に進む。他の動作は実施例１の図５と同じで説明を省略する。

【０１０５】また、受信動作について図１７を用いて説明する。本図は実施例１の図６と比較し、ステップ４６７、４６８をステップ４８７、４８９に置き換えてたもので、ステップ４８７で受信ＩＰパケット４４５の送信元ＩＰアドレスと暗号化情報テーブル２内の通信相手のＩＰアドレスとを比較し一致する通信相手のＩＰアドレスのが暗号化情報テーブル２内にあるかサーチして、一致するものがない場合は、復号せずステップ４６９に進む。一致するものがあれば、ステップ４８９に進み、その通信相手のＩＰアドレスに対応して登録しておいた受信用暗号鍵でＩＰパケット４４５のＩＰデータ部４１２を復号しステップ４６９に進む。他の動作は実施例１の図６と同じで説明を省略する。

【０１０６】次に、端末１ａと端末１ｂ間の送受信を例に暗号通信の動作を説明する。通信に先立ち図１５の暗号装置３ａの暗号化情報テーブル２ａに通信相手ＩＰアドレスに３１ｂ、送信用暗号鍵に３４１ｇ、受信用暗号鍵に３４１ｈの組を登録し、暗号装置３ｂの暗号化情報テーブル２ｂに通信相手ＩＰアドレスに３１ａ、送信用暗号鍵に３４１ｈ、受信用暗号鍵に３４１ｇの組を登録しておく。

【０１０７】そして、端末１ａにおいて送信元ＩＰアドレス３１ａ、宛先ＩＰアドレス３１ｂのＩＰパケット４４５を編集し、暗号装置３ａに渡すと、暗号装置３ａは宛先ＩＰアドレス３１ｂに対応する送信用暗号鍵３４１ｇで暗号化し、通信網９１ａに送信する。一方、暗号装置３ｂは通信網９１ａから送信元ＩＰアドレス３１ａ、宛先ＩＰアドレス３１ｂのＩＰパケットを受信すると送信元ＩＰアドレス３１ａに対応する受信用暗号鍵３４１ｇで復号し端末１ｂに渡す。次に端末１ｂが送信元ＩＰアドレス３１ｂ、宛先ＩＰアドレス３１ａ、のＩＰパケ

ット４４５を編集し、暗号装置３ｂに渡すと、暗号装置３ｂは送信元ＩＰアドレス３１ｂと宛先ＩＰアドレス３１ａの組に対応する暗号鍵３４１ｈで暗号化し、通信網９１ａに送信する。暗号装置３ａが通信網９１ａから送信元ＩＰアドレス３１ｂ、宛先ＩＰアドレス３１ａのＩＰパケット４４５を受信すると、送信元ＩＰアドレス３１ｂに対応する受信用暗号鍵３４１ｈで復号し端末１ａに渡す。

【０１０８】以上のように、端末１ａから端末１ｂに送信するときは暗号鍵３４１ｇを用い、逆に端末１ａが端末１ｂから受信するときは暗号鍵３４１ｈを用いるので送受信別の暗号鍵を用いて暗号通信ができる。従って、片方の暗号鍵が解読されても他方は解読されないので、従来例より暗号強度が増す。なお、本実施例では通信相手ＩＰアドレスに送信用暗号鍵と受信用暗号鍵を割り当てているが、実施例１のデータ種別と本実施例の通信相手ＩＰアドレスを組に対応して、送信用暗号鍵と受信用暗号鍵を割り当ててもよい。さらに、本実施例および上記の例で暗号鍵に実施例２の秘密鍵有効情報、第１暗号鍵、第２暗号鍵を割り当て暗号強度に応じた暗号化を行うこともでき、２つ以上の複数鍵を用いて複数回暗号化・復号してもよい。

【０１０９】また、上記実施例ではＴＣＰ／ＩＰの通信手順の場合について説明したが、ＩＰＸ（Internet Packet Exchange）やその他の通信手順であってもよく、上記実施例と同様の効果を奏する。また、端末１と暗号装置３は１対１に接続している例を示したが暗号装置３に複数台の端末１を接続しても同様の効果を奏する。次に、上記例では、通信相手のＩＰアドレスをもとに使用する暗号鍵を決めていたが、ＩＰアドレスの上位ビットが同一の端末でネットワークまたはサブネットワークを構成し、そのネットワーク内の各端末が同じ暗号鍵を用いて他の端末と暗号通信する場合は、ＩＰアドレスのネットワークを識別する上位桁をもとに暗号鍵を決めることもできる。

【０１１０】即ち、上記実施例の図１５の暗号化情報テーブル２の通信相手ＩＰアドレスと一致するものをサーチする場合、ＩＰアドレス一致の判定の代わりに図１８のネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。例えば、送信の場合は図１６のステップ４９５の通信相手ＩＰアドレス一致の判定の代わりに、ネットワークを識別する通信相手ＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。また、受信の場合は図１７のステップ４８７の通信相手ＩＰアドレス一致の判定の代わりに、図１８のネットワークを識別するＩＰアドレスの上位桁４０４を比較して一致の判定を行なう。他は上記実施例と同様である。以上のようにネットワーク対応に暗号鍵を割り当てれば、同じネットワークに属する端末には同じネットワークアドレスを登録すればよいので、端末ごと異なるＩＰアドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【０１１１】

【発明の効果】第一の発明においては、２つの端末間で、データ種別によって異なる暗号鍵を用いて通信できるので暗号強度が増す。

【０１１２】第二の発明においては、複数鍵を用いて複数回暗号化するので、暗号強度が増し、通信相手によって暗号化の回数と各回に用いる暗号鍵を選ぶことにより暗号強度を変えることができる。

【０１１３】第三の発明においては、データ種別ごとに異なる暗号鍵を使えるのでさらに暗号強度が増す。

【０１１４】第四の発明においては、送信元アドレスと宛先アドレスの組み合わせに対応して暗号鍵を割り当てるので、送信と受信に別々の暗号鍵で通信でき暗号強度が増す。

【０１１５】第六の発明においては、危険域の第１の通信網からの受信情報を復号して安全域の第２の通信網へ中継し、逆に安全域の端末から受信情報を暗号化して危険域に中継するので、安全域に属する複数の端末対応に暗号装置を設ける必要はなく、さらに暗号登録する必要もなく鍵の配布労力が省ける。

【０１１６】第七の発明においては、データ種別ごとに異なる暗号鍵を使えるのでさらに暗号強度が増す。

【０１１７】第八の発明においては、送信するときに用いる暗号鍵と受信するときに用いる暗号鍵を別にしたので、片方の暗号鍵が解読されても他方は解読されないので、従来例より暗号強度が増す。

【０１１８】第九の発明においては、送信と受信に別々にかつ、データ種別ごとに複数の暗号鍵を用いて複数回暗号化するのでさらに暗号強度が増す。

【０１１９】第十の発明においては、送信と受信に別々にかつ、複数の暗号鍵を用いて複数回暗号化するのでさらに暗号強度が増す。

【０１２０】第十一の発明においては、送信と受信に別々にかつ、データ種別ごとに異なる暗号鍵を使えるのでさらに暗号強度が増す。

【０１２１】第十二の発明においては、宛先対応に複数鍵を用いて複数回暗号化するので、暗号強度が増し、通信相手によって暗号化の回数と各回に用いる暗号鍵を選ぶことにより暗号強度を変えることができる。

【０１２２】第十三の発明においては、送信元アドレス、宛先アドレスとデータ種別の組み合わせに対応して複数鍵を割り当て複数回暗号化するので、暗号強度が増し、通信相手によって暗号化の回数と各回に用いる暗号鍵を選ぶことにより暗号強度を変えることができる。

【０１２３】第十四の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽

減できる。

【０１２４】第十五の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【０１２５】第十六の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【０１２６】第十七の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【０１２７】第十八の発明においては、端末アドレスの代わりに端末アドレスの一部で構成されるネットワークアドレスを登録すればよいので、端末ごと異なる端末アドレスの下位ビットを登録しなくてよく、操作労力を軽減できる。

【０１２８】

【図面の簡単な説明】

【図１】この発明の実施例１による暗号装置を示す構成図である。

【図２】この発明の実施例１による暗号通信システムを示す図である。

【図３】この発明の実施例１によるＩＰパケットの形式を示す図である。

【図４】この発明の実施例１による暗号化情報テーブルを示す図である。

【図５】この発明の実施例１による送信処理手順を示す図である。

【図６】この発明の実施例１による受信処理手順を示す図である。

【図７】この発明の実施例２による暗号化情報テーブルを示す図である。

【図８】この発明の実施例２による送信処理手順を示す図である。

【図９】この発明の実施例２による受信処理手順を示す図である。

【図１０】この発明の実施例３による暗号装置を示す構成図である。

【図１１】この発明の実施例３による暗号通信システムを示す図である。

【図１２】この発明の実施例３による暗号化情報テーブルを示す図である。

【図１３】この発明の実施例３による第２網側への中継処理手順を示す図である。

【図１４】この発明の実施例３による第１網側への中継処理手順を示す図である。

【図１５】この発明の実施例４による暗号化情報テーブルを示す図である。

【図１６】この発明の実施例４による送信処理手順を示す図である。

【図１７】この発明の実施例４による受信処理手順を示す図である。

【図１８】ＩＰアドレス構成を示す図である。

【図１９】従来の暗号装置を示す構成図である。

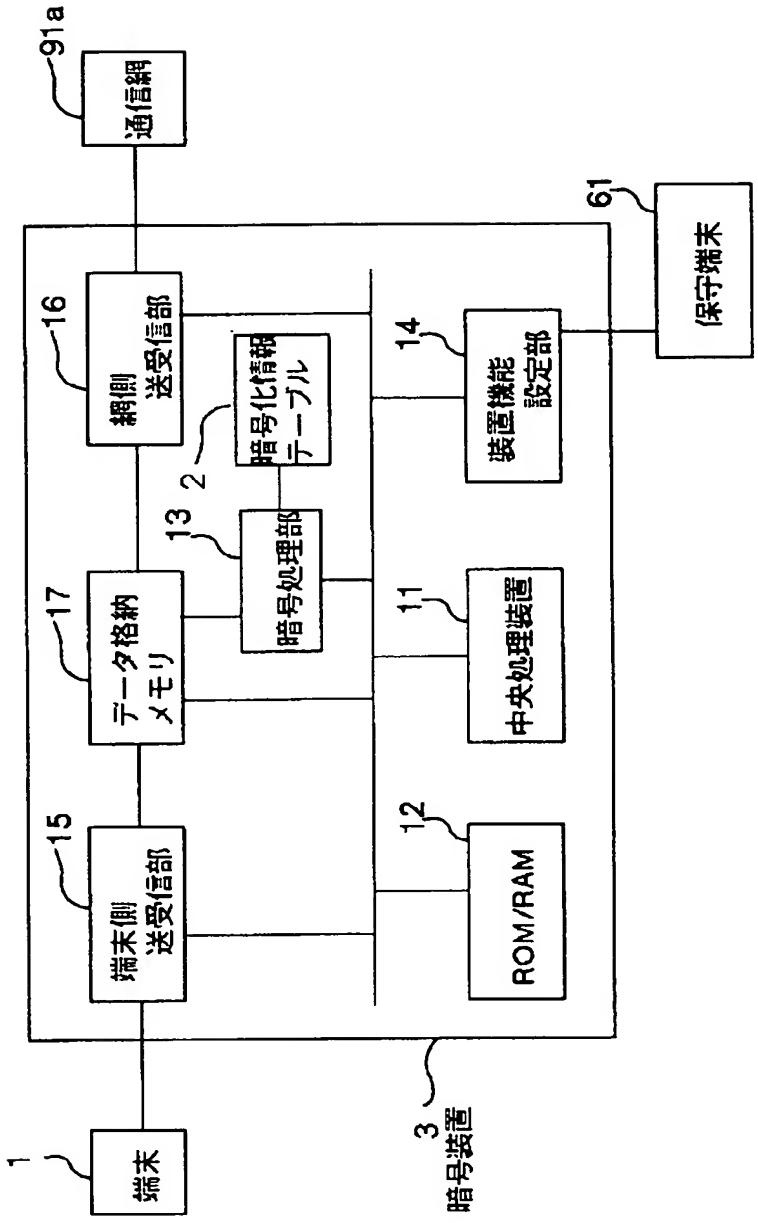
【図２０】従来の実施例による送信処理手順を示す図である。

【図２１】従来の実施例による受信処理手順を示す図である。

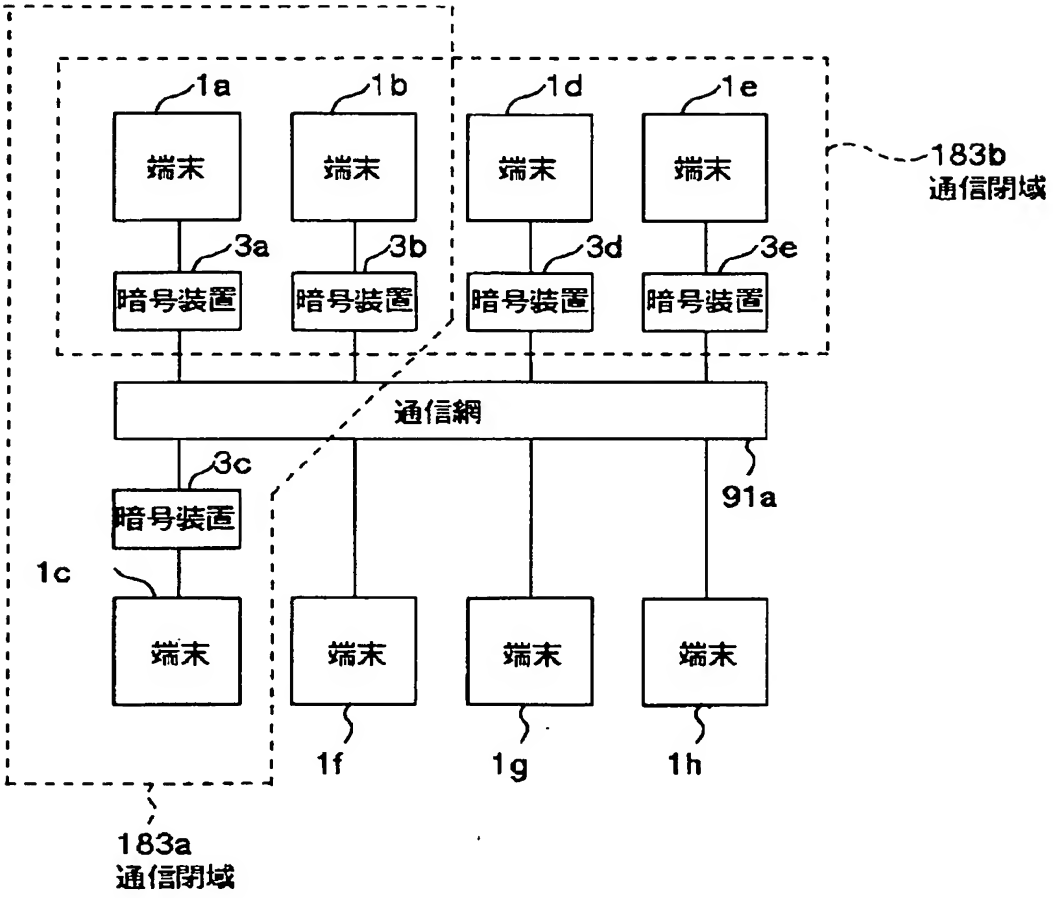
【符号の説明】

１１　中央処理装置
１２　ＲＯＭ／ＲＡＭ
１３　暗号処理部
１４　装置機能設定部
１５　端末側送受信部
１６　網側送受信部
１７　データ格納メモリ
１８　第２網側送受信部
３　暗号装置
３ａ～３ｅ　暗号装置
３ｍ　暗号装置
６１　保守端末
９１ａ　第１通信網
９１ｂ　第２通信網
１　端末
１ａ～１ｌ　端末
２ａ～２ｅ、２ｍ　暗号化情報テーブル
３１ａ～３１ｅ　ＩＰアドレス
３１ｉ～３１ｋ　ＩＰアドレス
３２６ａ～３２６ｂ　データ種別
３２７ａ～３２７ｃ　暗号鍵有効情報
３４１ａ～３４１ｎ　暗号鍵
４０１　送信元ＩＰアドレス部
４０２　宛先ＩＰアドレス部
４０４　ＩＰネットワークアドレス
４１１　ＩＰヘッダ部
４１２　ＩＰデータ部
４３１　データ種別部
４４１　ＴＣＰヘッダ部
４４２　ＴＣＰデータ部
４４５　ＩＰパケット

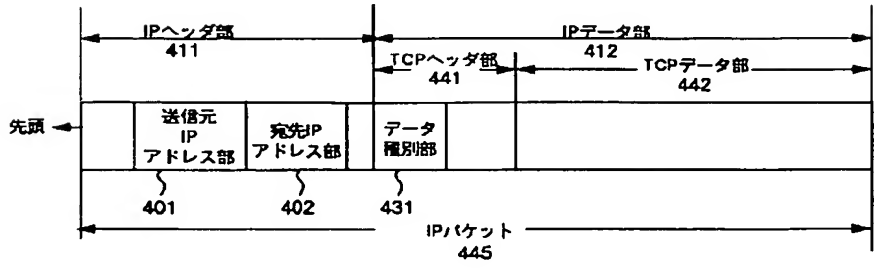
【図１】


91a
通信網
61
保守端末
16
網側
送受信部
暗号化情報
テーブル
2
14
装置機能
設定部
13
暗号処理部
17
データ格納
メモリ
11
中央処理装置
15
端末側
送受信部
12
ROM/RAM
1
端末
3
暗号装置

【図２】


1a
1b
1d
1e
端末
端末
端末
端末
183b
通信閉域
3a
3b
3d
3e
暗号装置
暗号装置
暗号装置
暗号装置
通信網
3c
91a
暗号装置
1c
端末
端末
端末
端末
1f
1g
1h
183a
通信閉域

【図３】


IPヘッダ部
411
IPデータ部
412
TCPヘッダ部
441
TCPデータ部
442
先頭
送信元
IP
アドレス部
宛先IP
アドレス部
データ
種別部
401
402
431
IPパケット
445

【図４】

IPアドレス	データ種別	暗号鍵
31b	326a	341a
31b	326b	341b
31c	326a	341a
31d	326b	341b
31e	326b	341b

2a 暗号化情報テーブル

IPアドレス	データ種別	暗号鍵
31a	326a	341a
31c	326a	341a
31a	326b	341b
31d	326b	341b
31e	326b	341b

2b 暗号化情報テーブル

IPアドレス	データ種別	暗号鍵
31a	326a	341a
31b	326a	341a

2c 暗号化情報テーブル

IPアドレス	データ種別	暗号鍵
31a	326b	341b
31b	326b	341b
31e	326b	341b

2d 暗号化情報テーブル

IPアドレス	データ種別	暗号鍵
31a	326b	341b
31b	326b	341b
31d	326b	341b

2e 暗号化情報テーブル

【図７】

IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31b	327a	341c	341d
31c	327b	341c	—
31d	327c	—	341d
31e	327c	—	341d

2a 暗号化情報テーブル

IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31a	327a	341c	341d
31c	327b	341c	—
31d	327c	—	341d
31e	327c	—	341d

2b 暗号化情報テーブル

IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31a	327b	341c	—
31b	327b	341c	—

2c 暗号化情報テーブル

IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31a	327c	—	341d
31b	327c	—	341d
31e	327c	—	341d

2d 暗号化情報テーブル

IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31a	327c	—	341d
31b	327c	—	341d
31d	327c	—	341d

2e 暗号化情報テーブル

【図１２】

IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31b	327b	341e	—
31l	327b	341e	—

2a 暗号化情報テーブル

IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31a	327b	341e	—
31l	327b	341e	—

2b 暗号化情報テーブル

IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31j	327b	341f	—
31k	327b	341f	—

2e 暗号化情報テーブル

2m 暗号化情報テーブル

第1網側IPアドレス	第2網側IPアドレス	暗号鍵有効情報	第1暗号鍵	第2暗号鍵
31a	31i	327b	341e	—
31b	31l	327b	341e	—
31e	31j	327b	341f	—
31e	31k	327b	341f	—

【図１５】

通信相手IPアドレス	送信用暗号鍵	受信用暗号鍵
31b	341g	341h
31c	341i	341j

2a 暗号化情報テーブル

通信相手IPアドレス	送信用暗号鍵	受信用暗号鍵
31a	341h	341g
31c	341k	341l

2b 暗号化情報テーブル

通信相手IPアドレス	送信用暗号鍵	受信用暗号鍵
31e	341j	341l
31b	341l	341k

2c 暗号化情報テーブル

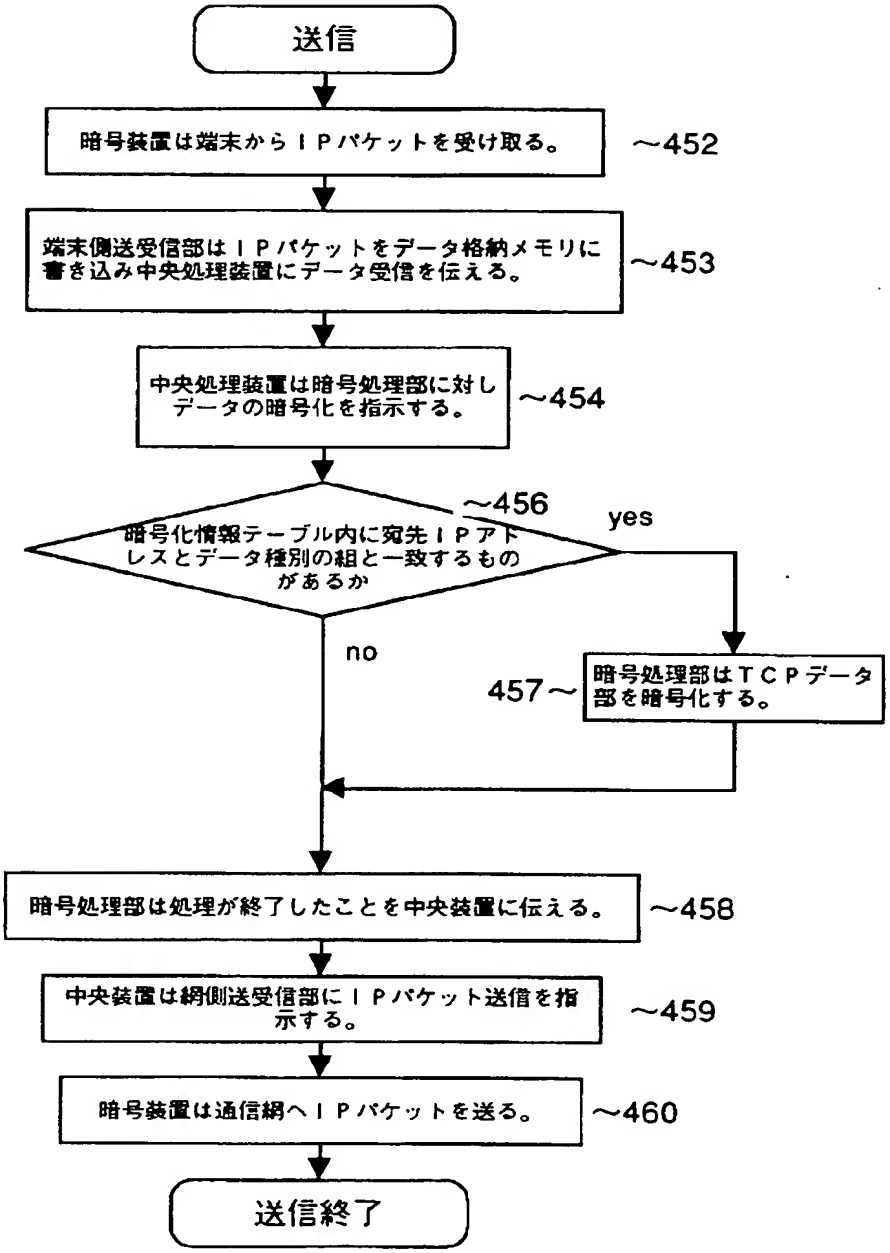
通信相手IPアドレス	送信用暗号鍵	受信用暗号鍵
31e	341n	341m

2d 暗号化情報テーブル

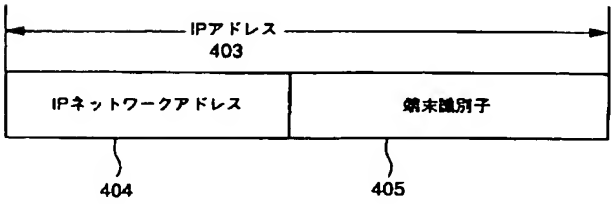
通信相手IPアドレス	送信用暗号鍵	受信用暗号鍵
31d	341m	341n

2e 暗号化情報テーブル

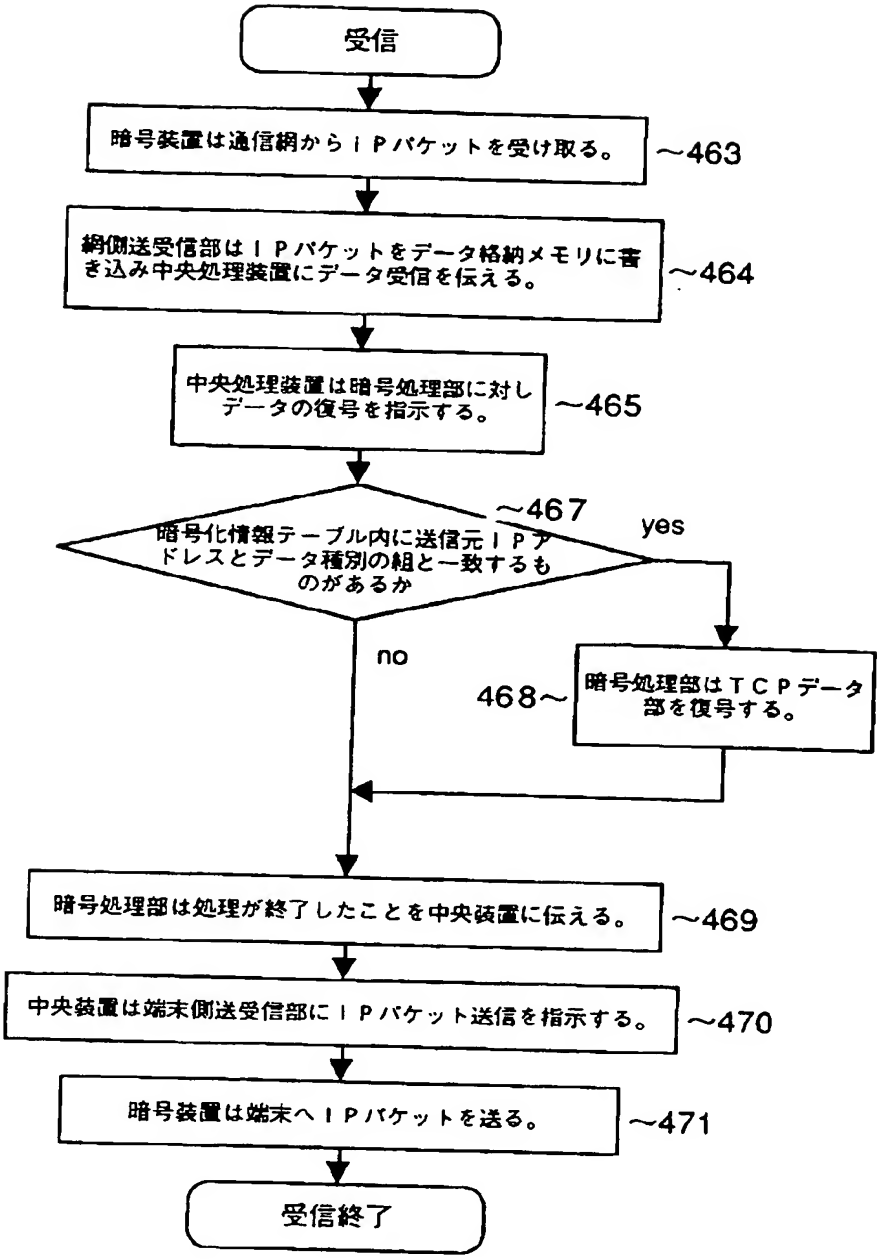
【図５】


送信
暗号装置は端末からＩＰパケットを受け取る。
～452
端末側送受信部はＩＰパケットをデータ格納メモリに書き込み中央処理装置にデータ受信を伝える。
～453
中央処理装置は暗号処理部に対しデータの暗号化を指示する。
～454
～456
暗号化情報テーブル内に宛先ＩＰアドレスとデータ種別の組と一致するものがあるか
yes
no
457～
暗号処理部はＴＣＰデータ部を暗号化する。
暗号処理部は処理が終了したことを中央装置に伝える。
～458
中央装置は網側送受信部にＩＰパケット送信を指示する。
～459
暗号装置は通信網へＩＰパケットを送る。
～460
送信終了

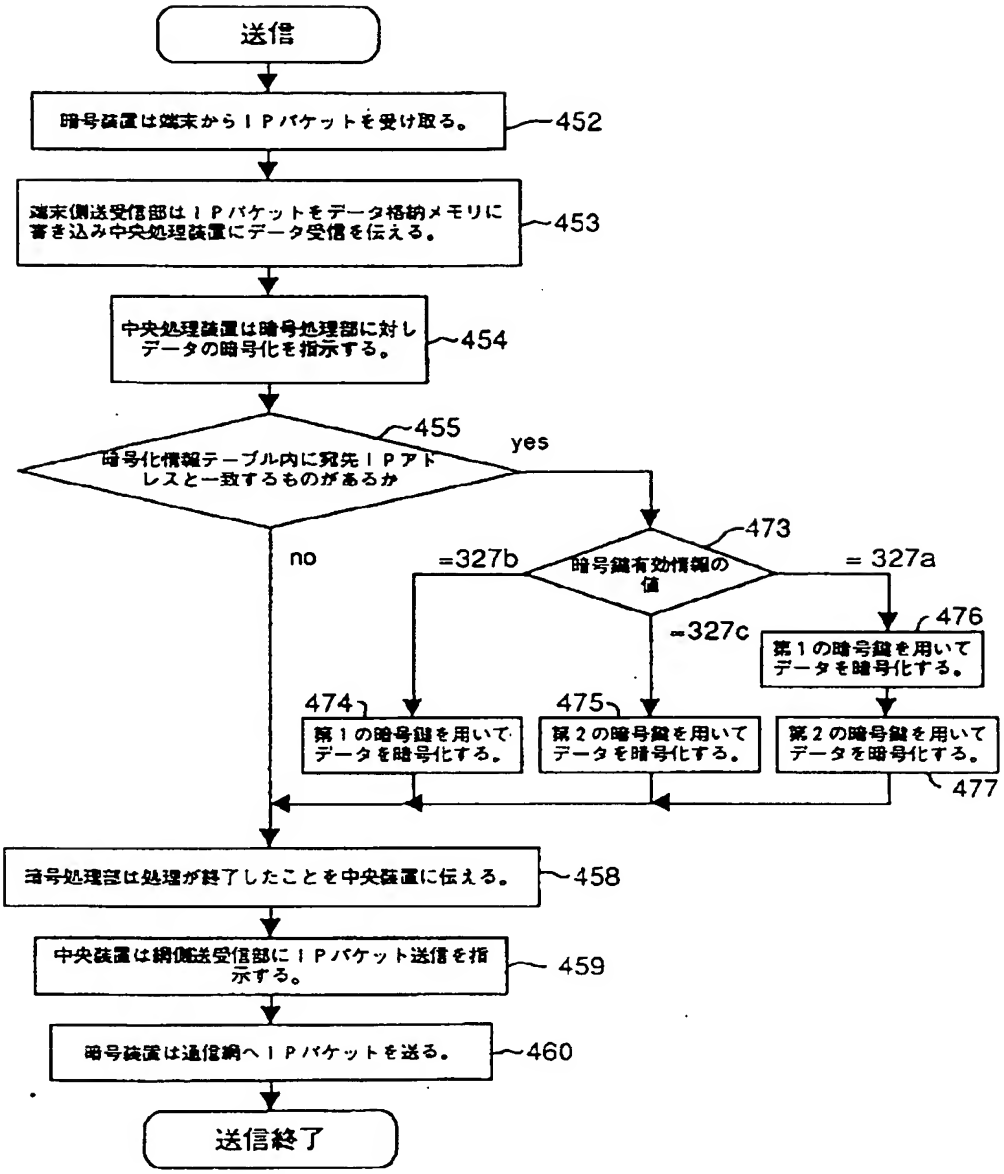
【図１８】


IPアドレス
403
IPネットワークアドレス
端末識別子
404
405

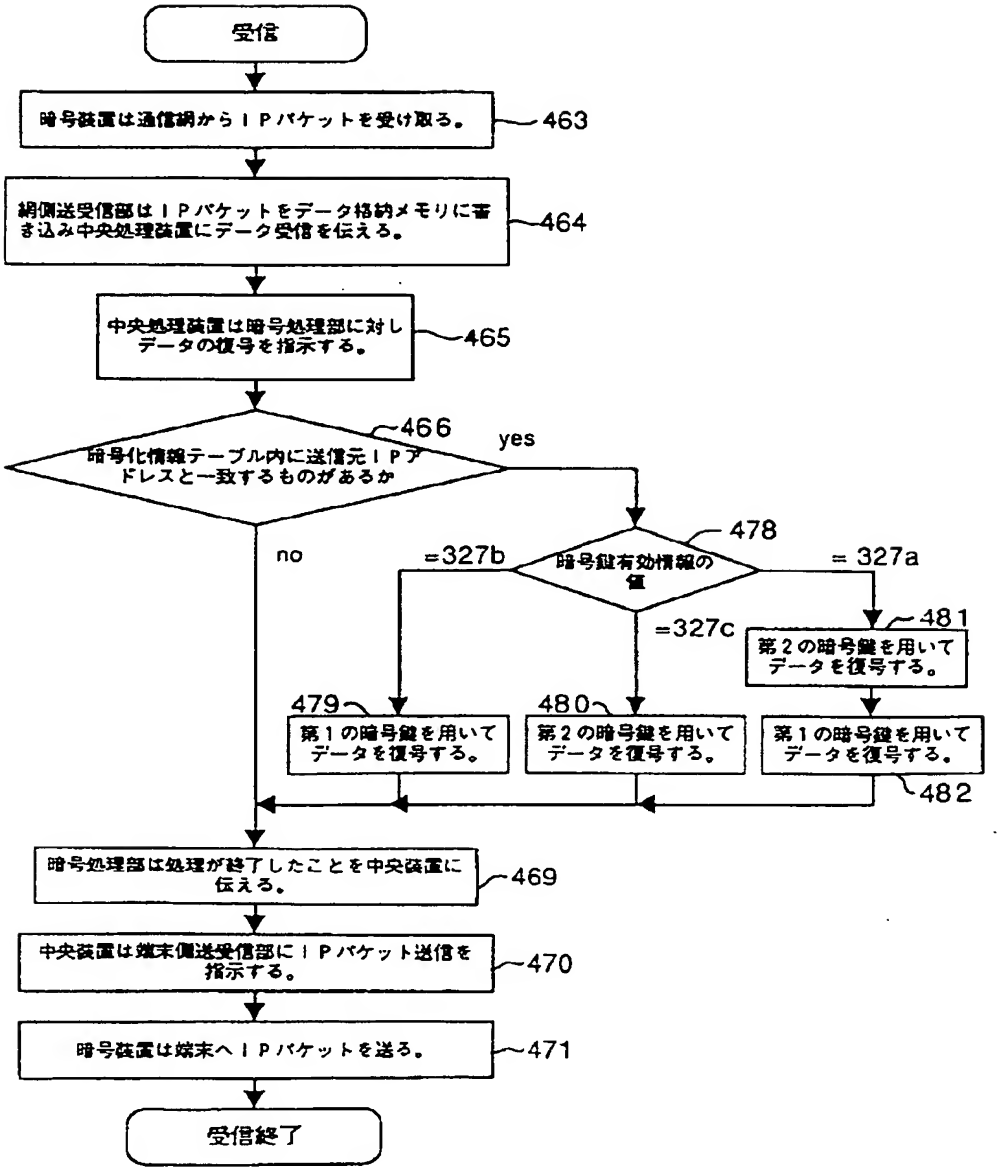
【図６】


受信
暗号装置は通信網からＩＰパケットを受け取る。
～463
網側送受信部はＩＰパケットをデータ格納メモリに書き込み中央処理装置にデータ受信を伝える。
～464
中央処理装置は暗号処理部に対しデータの復号を指示する。
～465
～467
暗号化情報テーブル内に送信元ＩＰアドレスとデータ種別の組と一致するものがあるか
yes
no
468～
暗号処理部はＴＣＰデータ部を復号する。
暗号処理部は処理が終了したことを中央装置に伝える。
～469
中央装置は端末側送受信部にＩＰパケット送信を指示する。
～470
暗号装置は端末へＩＰパケットを送る。
～471
受信終了

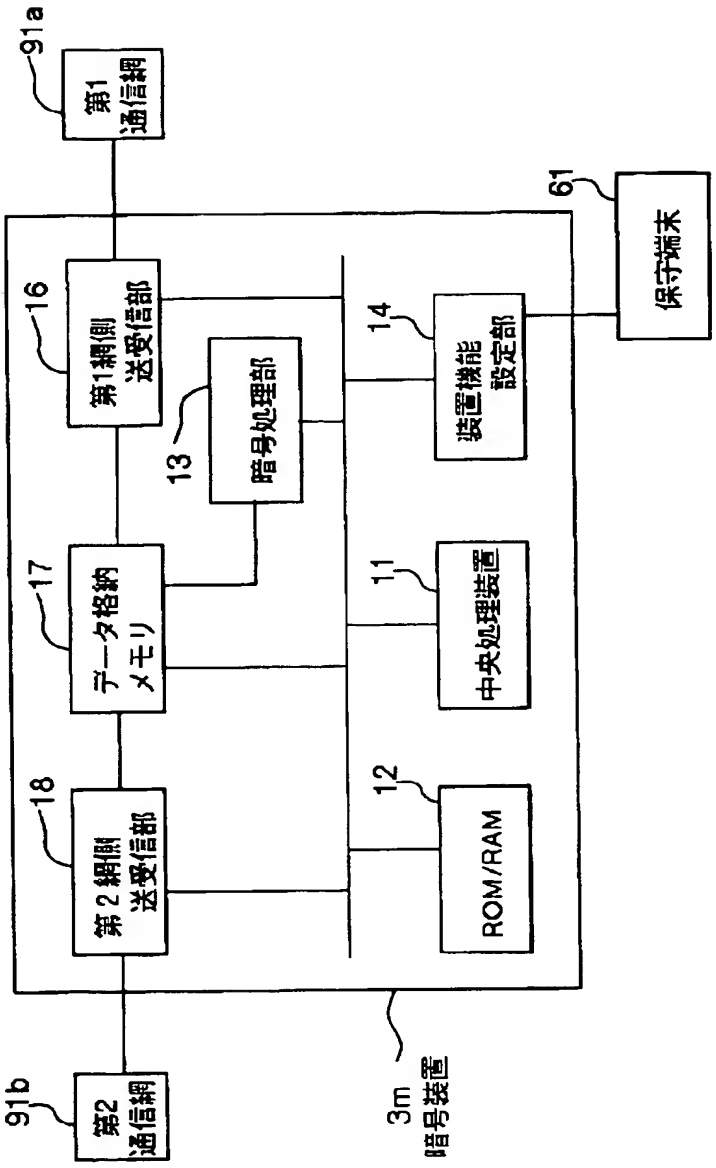
【図８】


送信
暗号装置は端末からＩＰパケットを受け取る。
452
端末側送受信部はＩＰパケットをデータ格納メモリに書き込み中央処理装置にデータ受信を伝える。
453
中央処理装置は暗号処理部に対しデータの暗号化を指示する。
454
455
暗号化情報テーブル内に宛先ＩＰアドレスと一致するものがあるか
yes
no
473
暗号鍵有効情報の値
=327b
=327c
= 327a
476
第１の暗号鍵を用いてデータを暗号化する。
474
第１の暗号鍵を用いてデータを暗号化する。
475
第２の暗号鍵を用いてデータを暗号化する。
第２の暗号鍵を用いてデータを暗号化する。
477
暗号処理部は処理が終了したことを中央装置に伝える。
458
中央装置は網側送受信部にＩＰパケット送信を指示する。
459
暗号装置は通信網へＩＰパケットを送る。
460
送信終了

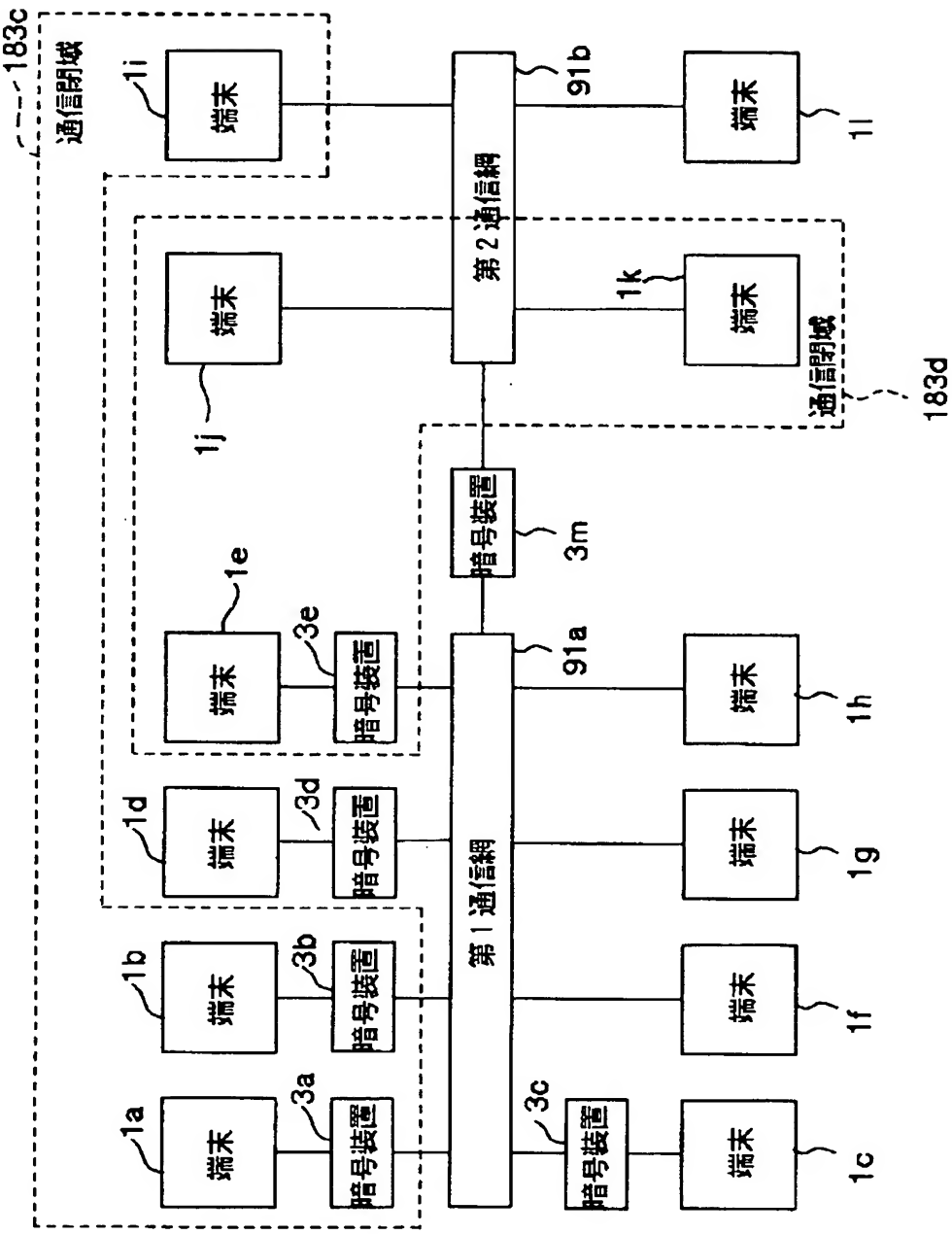
【図９】


受信
暗号装置は通信網からＩＰパケットを受け取る。
463
網側送受信部はＩＰパケットをデータ格納メモリに書き込み中央処理装置にデータ受信を伝える。
464
中央処理装置は暗号処理部に対しデータの復号を指示する。
465
466
暗号化情報テーブル内に送信元ＩＰアドレスと一致するものがあるか
yes
no
478
暗号鍵有効情報の値
=327b
=327c
= 327a
481
第２の暗号鍵を用いてデータを復号する。
479
第１の暗号鍵を用いてデータを復号する。
480
第２の暗号鍵を用いてデータを復号する。
第１の暗号鍵を用いてデータを復号する。
482
暗号処理部は処理が終了したことを中央装置に伝える。
469
中央装置は端末側送受信部にＩＰパケット送信を指示する。
470
暗号装置は端末へＩＰパケットを送る。
471
受信終了

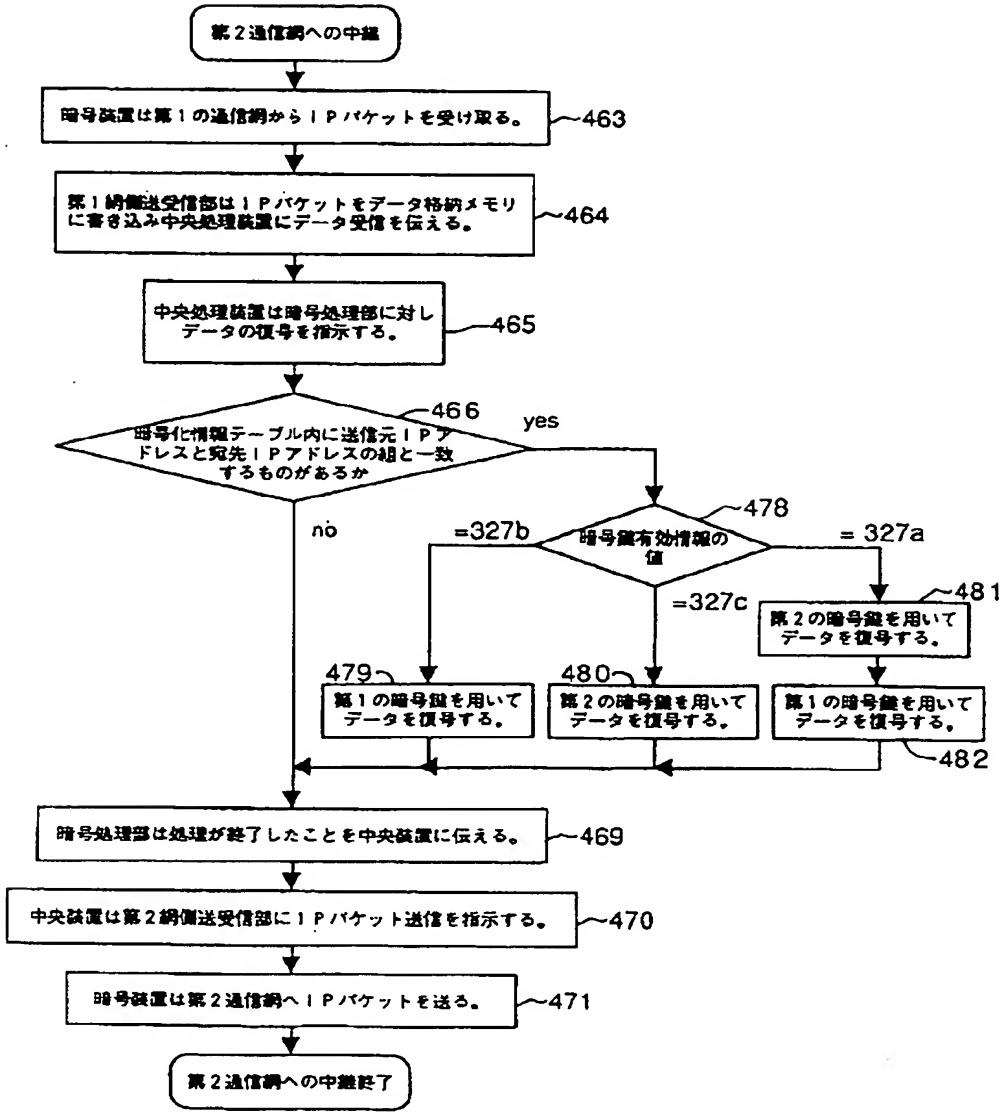
【図１０】


91a
第1
通信網
61
保守端末
16
第1網側
送受信部
14
装置機能
設定部
13
暗号処理部
17
データ格納
メモリ
11
中央処理装置
18
第2網側
送受信部
12
ROM/RAM
91b
第2
通信網
3m
暗号装置

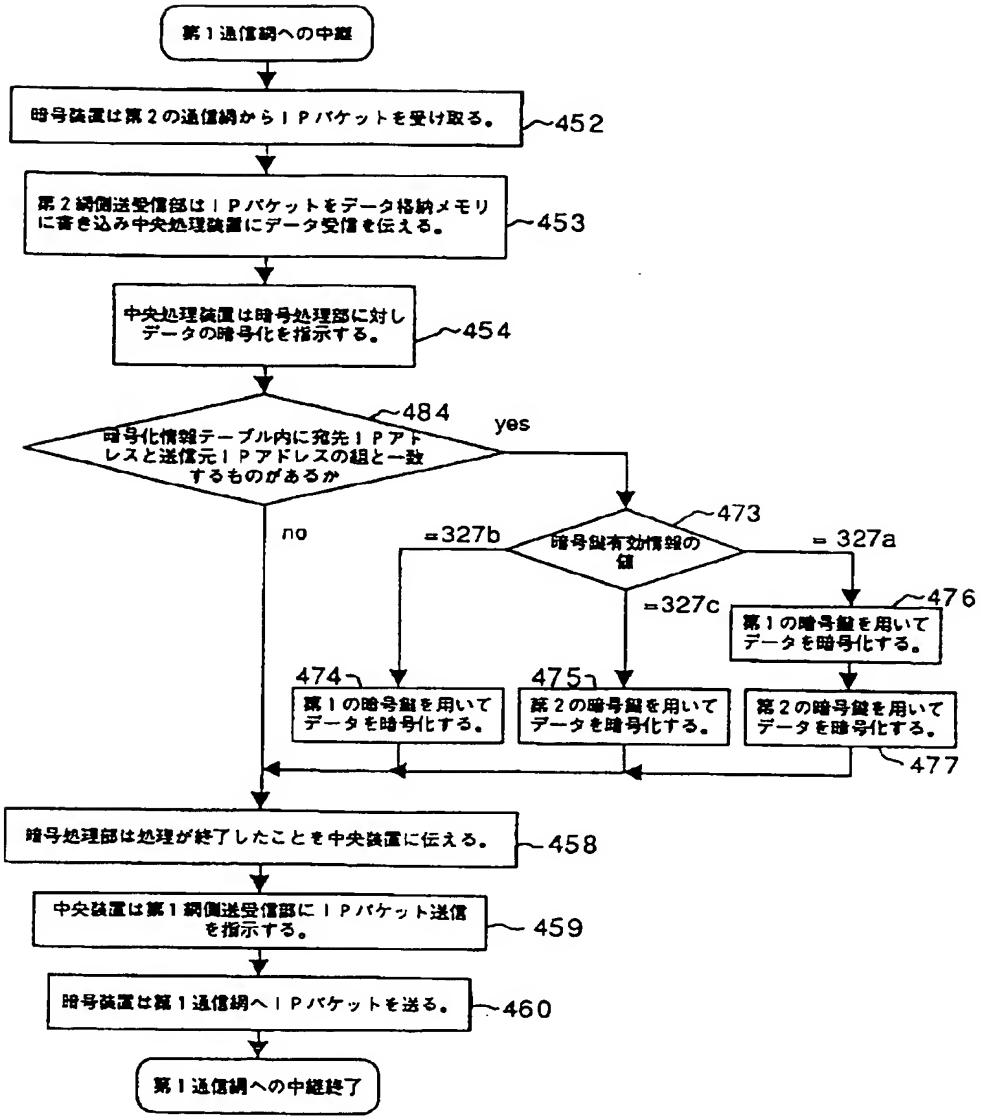
【図１１】


183c
通信閉域
1i
端末
91b
端末
1l
第２通信網
1j
端末
1k
端末
通信閉域
183d
暗号装置
3m
1e
端末
3e
暗号装置
91a
端末
1h
1d
端末
3d
暗号装置
第１通信網
端末
1g
1b
端末
3b
暗号装置
端末
1f
1a
端末
3a
暗号装置
3c
暗号装置
端末
1c

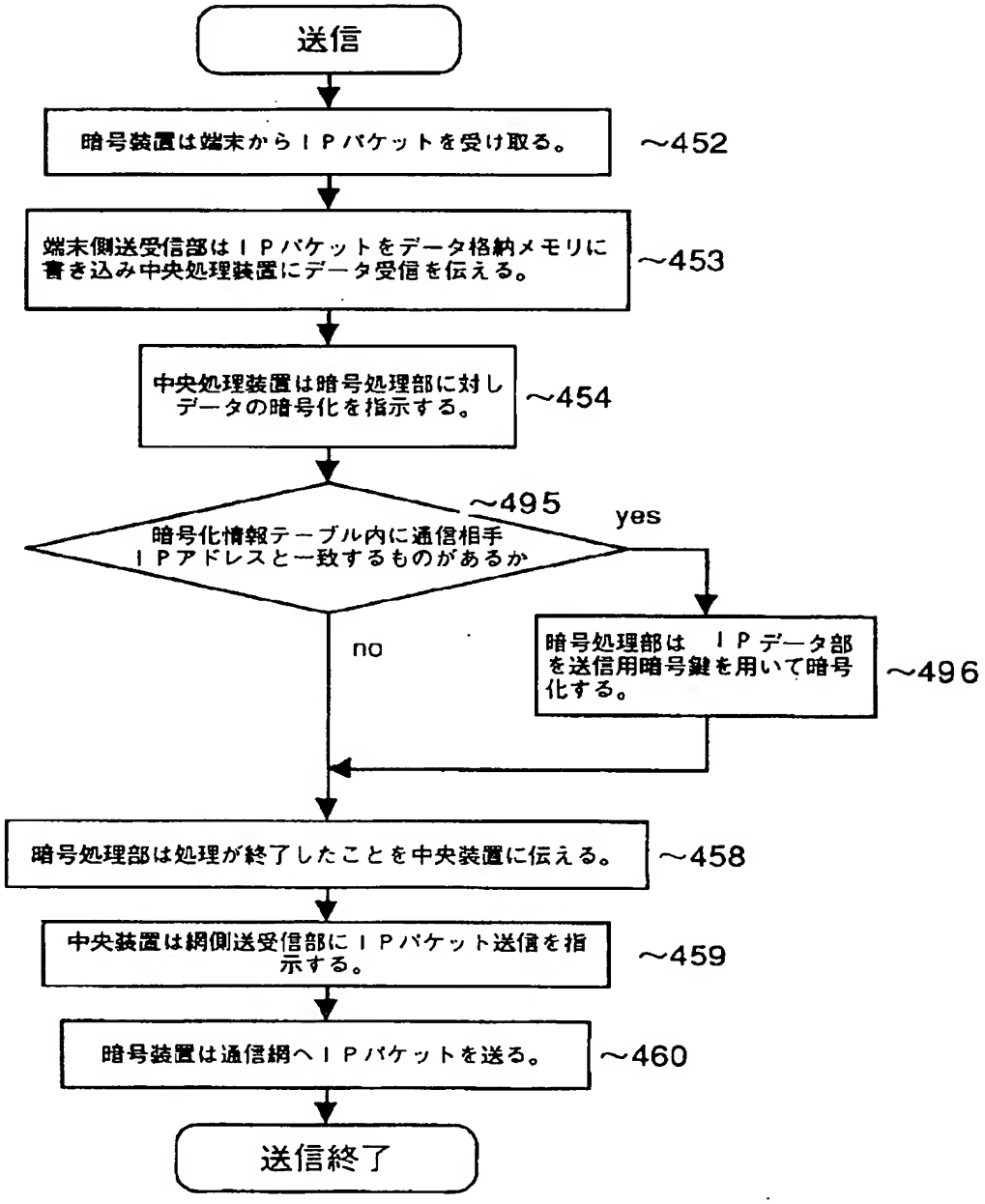
【図１３】


第２通信網への中継
暗号装置は第１の通信網からＩＰパケットを受け取る。
463
第１網側送受信部はＩＰパケットをデータ格納メモリに書き込み中央処理装置にデータ受信を伝える。
464
中央処理装置は暗号処理部に対しデータの復号を指示する。
465
暗号化情報テーブル内に送信元ＩＰアドレスと宛先ＩＰアドレスの組と一致するものがあるか
466
yes
no
暗号鍵有効情報の値
478
=327b
=327c
= 327a
第２の暗号鍵を用いてデータを復号する。
481
第１の暗号鍵を用いてデータを復号する。
479
第２の暗号鍵を用いてデータを復号する。
480
第１の暗号鍵を用いてデータを復号する。
482
暗号処理部は処理が終了したことを中央装置に伝える。
469
中央装置は第２網側送受信部にＩＰパケット送信を指示する。
470
暗号装置は第２通信網へＩＰパケットを送る。
471
第２通信網への中継終了

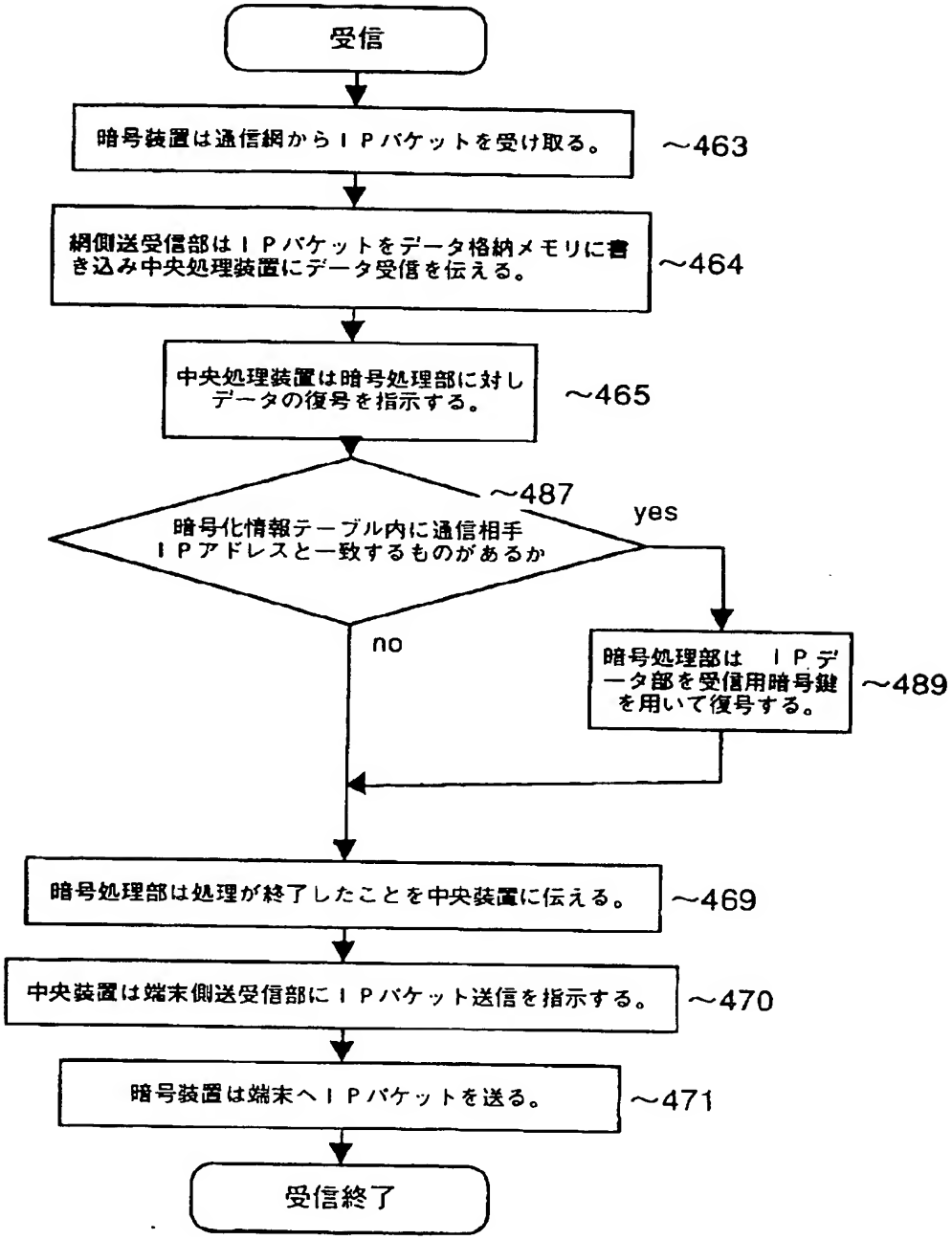
【図１４】


第１通信網への中継
暗号装置は第２の通信網からＩＰパケットを受け取る。
452
第２網側送受信部はＩＰパケットをデータ格納メモリに書き込み中央処理装置にデータ受信を伝える。
453
中央処理装置は暗号処理部に対しデータの暗号化を指示する。
454
暗号化情報テーブル内に宛先ＩＰアドレスと送信元ＩＰアドレスの組と一致するものがあるか
484
yes
no
暗号鍵有効情報の値
473
=327b
=327c
= 327a
第１の暗号鍵を用いてデータを暗号化する。
474
第２の暗号鍵を用いてデータを暗号化する。
475
第２の暗号鍵を用いてデータを暗号化する。
476
477
暗号処理部は処理が終了したことを中央装置に伝える。
458
中央装置は第１網側送受信部にＩＰパケット送信を指示する。
459
暗号装置は第１通信網へＩＰパケットを送る。
460
第１通信網への中継終了

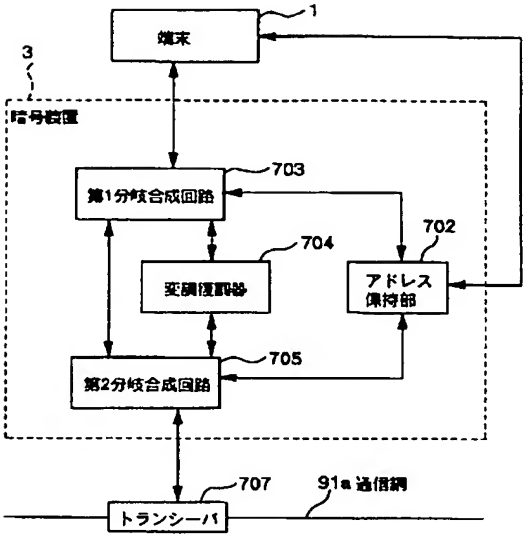
【図１６】


送信
暗号装置は端末からＩＰパケットを受け取る。
～452
端末側送受信部はＩＰパケットをデータ格納メモリに書き込み中央処理装置にデータ受信を伝える。
～453
中央処理装置は暗号処理部に対しデータの暗号化を指示する。
～454
～495
暗号化情報テーブル内に通信相手ＩＰアドレスと一致するものがあるか
yes
no
暗号処理部はＩＰデータ部を送信用暗号鍵を用いて暗号化する。
～496
暗号処理部は処理が終了したことを中央装置に伝える。
～458
中央装置は網側送受信部にＩＰパケット送信を指示する。
～459
暗号装置は通信網へＩＰパケットを送る。
～460
送信終了

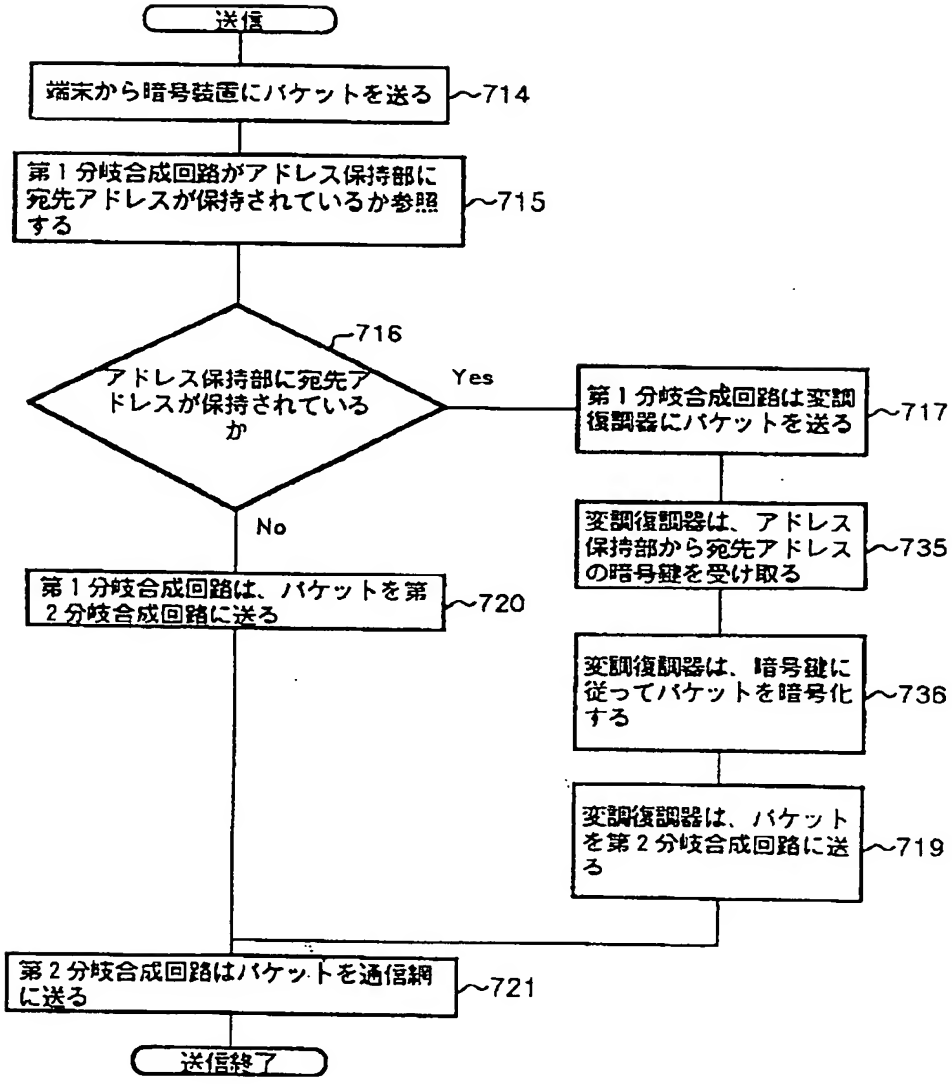
【図１７】


受信
暗号装置は通信網からＩＰパケットを受け取る。
～463
網側送受信部はＩＰパケットをデータ格納メモリに書き込み中央処理装置にデータ受信を伝える。
～464
中央処理装置は暗号処理部に対しデータの復号を指示する。
～465
～487
暗号化情報テーブル内に通信相手ＩＰアドレスと一致するものがあるか
yes
no
暗号処理部はＩＰデータ部を受信用暗号鍵を用いて復号する。
～489
暗号処理部は処理が終了したことを中央装置に伝える。
～469
中央装置は端末側送受信部にＩＰパケット送信を指示する。
～470
暗号装置は端末へＩＰパケットを送る。
～471
受信終了

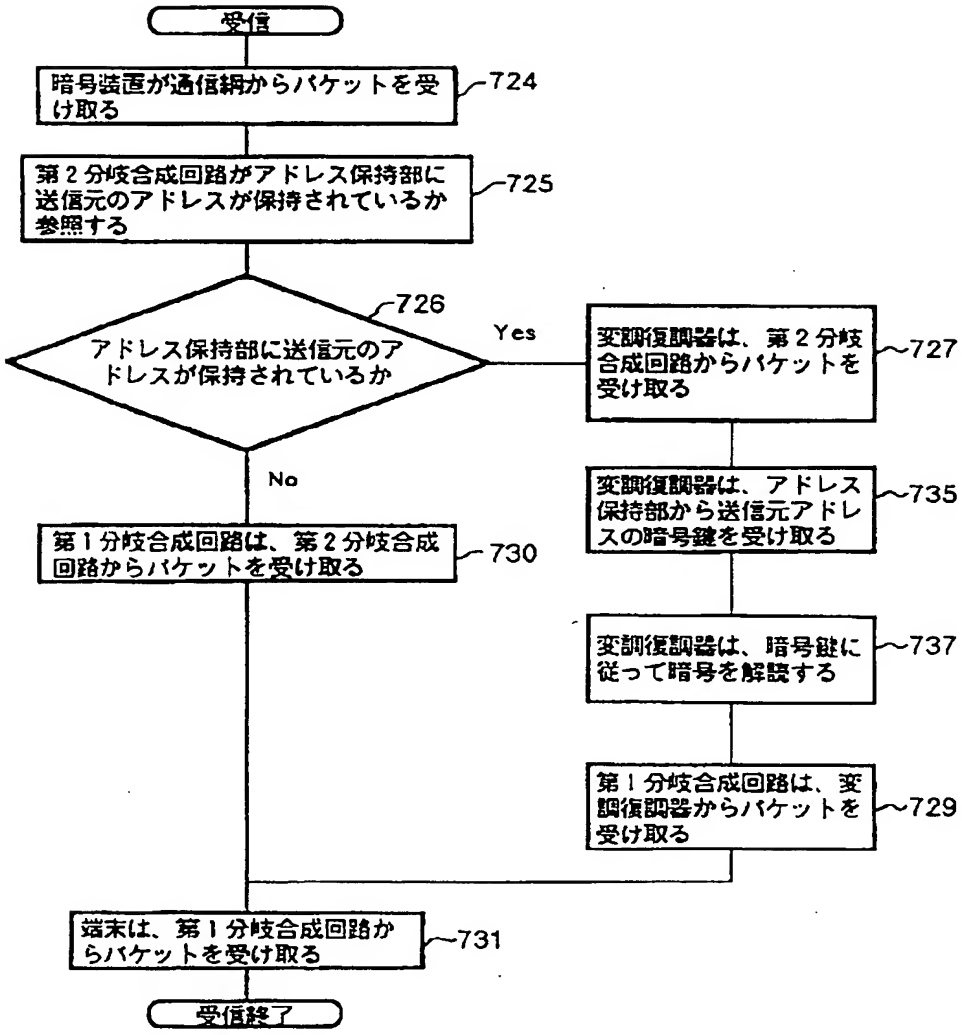
【図１９】


1
端末
3
信号装置
703
第1分岐合成回路
702
704
変調復調部
アドレス
保持部
705
第2分岐合成回路
707
91a 通信網
トランシーバ

【図２０】


送信
端末から暗号装置にパケットを送る
714
第１分岐合成回路がアドレス保持部に宛先アドレスが保持されているか参照する
715
716
アドレス保持部に宛先アドレスが保持されているか
Yes
No
第１分岐合成回路は変調復調器にパケットを送る
717
変調復調器は、アドレス保持部から宛先アドレスの暗号鍵を受け取る
735
変調復調器は、暗号鍵に従ってパケットを暗号化する
736
変調復調器は、パケットを第２分岐合成回路に送る
719
第１分岐合成回路は、パケットを第２分岐合成回路に送る
720
第２分岐合成回路はパケットを通信網に送る
721
送信終了

【図２１】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		7259－5Ｊ		

(72)発明者　横山　幸雄
鎌倉市大船五丁目１番１号　三菱電機株式会社通信システム研究所内

(72)発明者　永島　規充
鎌倉市大船五丁目１番１号　三菱電機株式会社通信システム研究所内